Multinational Information Sharing (MNIS)
Protection Profile (PP)
For
Networked Information Systems

Version 1.0

25 September 2002

Foreword

This system level Protection Profile (PP) was developed at the request of many U.S. war-fighting Commands. Each Command expressed a need for information system capabilities that support information sharing between U.S. and foreign partners engaged in multinational operations. The intent of this PP is to establish system-level functional security and assurance requirements for these capabilities. Multinational Information Sharing (MNIS) is defined as the sharing of information among multiple national partners that have formed a coalition or alliance to address some specific purpose. Today, every Combatant Command, Service, and Agency (C/S/A) has requirements to share information among multinational partners. This PP establishes system-level functional and assurance requirements to enable the sharing to take place as securely as presently possible and practical.

The audience for this protection profile will be the system architects and engineers, developers, vendors, maintainers, and certification authorities of MNIS systems and products. For example, System Security Engineers (SSEs) will find the system level requirements in this PP useful in their efforts to respond to various specific operational requirements and complete detailed system security engineering leading to the selection and certification of products and systems to support MNIS solutions.

This PP is based on the *Common Criteria (CC) for Information Technology Security Evaluations*, Version 2.1, August 1999. Further information on the CC can be found on the Internet at http://www.commoncriteria.org/ and http://niap.nist.gov/. Information about Protection Profiles can be found on the Internet at http://www.iatf.net/.

Comments on this MNIS Protection Profile should be directed to:

Director National Security Agency
Attn: V21 Information System Security Engineering
Suite #6730
9800 Savage Road
Ft. George G. Meade, Md. 20755

Executive Summary

This system level Protection Profile (PP) outlines functional and assurance security requirements for sharing information classified up to the Secret level among multinational partners. The PP proposes a multinational information sharing (MNIS) model that provides a capability for the multinational partners to work together in a collaborative environment. The assumption is that the mission operation is conducted from the collaborative multinational environment. In the MNIS model, the high-collaboration environment connects to individual Secret-level partner environments, which typically already exist. See figure 1, page 21. This interconnection permits communications between partner national environments and team members assigned to the collaborative environment.

This high-collaboration multinational environment has four key characteristics:

- The information systems in the multinational environment operate at a "multinational Secret system high" level with high assurance boundary protection between the multinational environment and each of the partner environments (including the U.S.).
- Communities of interest (COIs), protected by medium robustness security methods, can exist within the system high multinational security domain. COIs might be based on mission roles or user responsibilities.
- The multinational environment can be spread across a number of physically separate yet interconnected enclaves. See figure 2, page 25.
- The U.S or its agent manages the infrastructure of the multinational environment (including security administration). Administration of the multinational environment is split between two roles: Security Administrator and System Administrator.

Operating at a system high level provides for a high level of operational collaboration via the use of commercial technologies. Specifically, medium robustness commercial capabilities are sufficient to control access to the COI information *within the multinational information domain.* (High-assurance security technologies are required to control the flow of information into and out of the multinational information domain.) As a result, a coalition or alliance can collaboratively plan, execute, and monitor an operation as an integrated team, yet team members with certain roles (such as network administration or special operations) can restrict access to their COI information via the commercially-available security services.

Analysis Approach

This protection profile presents a generic set of multinational operational requirements from which the authors developed a model for multinational information sharing. Using the model, the PP presents an analysis of the flow of information into and out of the collaborative multinational environment and between users within the collaborative multinational environment. Information flow is described in operational terms and in high-level technical terms. To assist the reader in understanding the operational capabilities provided by these flows

of data, Appendix D provides four operational scenarios that depend on securely sharing information. These scenarios are:

- Report Composition Utilizing Multiple Information Domains
- Report Distribution to Multiple Information Domains
- Collaboration Among the U.S. and Its Partners
- Automatic Feeds Between Different Information Domains

The MNIS PP is a system-of-systems profile rather than a component protection profile. It describes the security requirements for a capability that incorporates many components and subsystems. Instead of listing requirements for all of the components, the PP outlines four broad categories of security functionality that are necessary for secure multinational information sharing. These categories are Access Control, Cross-Domain Filtering, Security Administration, and Transmission Security. This protection profile provides the security requirements for each category instead of for the entire system-of-systems or for each component that might conceivably be implemented in a specific multinational operation. System architects, developers, and accreditors can apply the requirements in this PP to specific multinational capabilities that they may implement.

Functional and Assurance Requirements

The security functional requirements are given for each of the categories of security functionality. (See Chapter 5.) However, requirements for Transmission Security mechanisms are already available from other sources. Therefore, this PP includes those sources by reference instead of duplicating them in the text of the PP.

Similarly, this PP presents security assurance requirements for three of the categories of security functionality, excluding Transmission Security. Because of the robustness required in the Cross-Domain Filtering category, the evaluated assurance level (EAL) for this category is EAL 5 Augmented. The EAL for the Access Control and Security Administration categories is EAL 4 Augmented. See Section 6.4 for the rationale that supports these EALs.

Additional Features of the MNIS Protection Profile

The multinational enclave in the MNIS model is designed to operate at a single security level that is protected at the Secret level, with all information releasable to all multinational partners. The medium robustness security functionality within the MNIS enclave is not designed to provide sufficient robustness to protect bilateral and non-releasable information from the other partners.

The U.S. is expected to manage and administer the MNIS environment and enforce the security policy that is negotiated among the multinational partners. The U.S. combatant commander is allowed to authorize a contractor or a trusted partner to manage the MNIS environment. The administrative functions for the multinational information systems are split into a security

administrator and a system administrator to provide checks and balances and to reduce the possibility that a single individual can gain unrestricted system control.

Document Organization

Chapter 1 provides the introductory material for the MNIS PP.

Chapter 2 provides a description of the Target of Evaluation (TOE).

Chapter 3 provides a discussion of the expected TSE. It defines the set of assumptions used in generating the MNIS PP, the threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware or software, or through the environmental controls. It also defines the security policies to be enforced by the TOE.

Chapter 4 defines the security objectives for both the TOE and the TSE.

Chapter 5 contains the functional and assurance requirements derived from the CC, Parts 2 and 3, respectively, that the TOE must satisfy. Application notes are included with the components whenever it was felt that additional clarification of the requirements was necessary.

Chapter 6 provides rationale for each threat, policy, security objective, and security requirement. It explains how the set of requirements is complete relative to the objectives, and that each security objective is addressed by one or more component requirements. It provides an analysis of the dependencies between component requirements and proposes the strength of function and evaluated assurance level for the TOE.

Appendices provide an acronym list, references, a glossary of common terms, and a set of operational scenarios used during the analysis of data flows between information domains in the multinational information sharing model.

Table of Contents

List of Figures

Please note that color is used in figures 2, 6, and 7 to draw attention to characteristics or to identify differences. When these figures are printed in black and white, the loss of color may make it difficult to discern these characteristics or differences. We apologize for any inconvenience.

List of Tables

1 - Introduction

1.1 Background

This Protection Profile (PP) was generated under the Information Assurance Solutions program, sponsored by the National Security Agency (NSA). The Information System Security Organization of NSA initiated this effort in response to Department of Defense (DoD), Combatant Command, Service, and Agency (C/S/A) expressed requirements to establish a security standard for networked information system solutions that are targeted at supporting multinational information sharing (MNIS) operations.

1.2 Identification

Title: Multinational Information Sharing (MNIS) Protection Profile (PP)

Authors: Mike Sheridan, National Security Agency
Rob Simmons, The MITRE Corporation
Eliot Sohmer, ACS Defense, Incorporated

Contributors: Horace Boner, Booz-Allen and Hamilton
Russ Bowmar, National Security Agency
Jeanne S. Firey, The MITRE Corporation
Ronald A. Jeter, National Security Agency
Richard Staiger, National Security Agency

Vetting Status: Pending
CC Version: 2.1 [ISO/IEC-15408: 1999]
Registration: <to be filled in by registry>
Keywords: Access Control, Coalition, Communities of Interest, Cross-Domain Filtering, Multinational Military Operations, Multiple Security Levels, Secure Information Sharing, Security Administration, Split Administration, and Transmission Security.

1.3 Protection Profile Overview

According to *Joint Vision 2020*, the United States military must be prepared to operate with multinational partners. Not surprisingly, each Combatant Commander has stated a need for information sharing in support of multinational operations. Multinational operations can be a consequence of bilateral or multilateral agreements, coalition activity, or alliance responsibilities. U.S. military forces must be prepared to interoperate with multinational forces and be able to coordinate military operations, as necessary, with government agencies and international

organizations.[1] Therefore, the term "multinational partner" also can refer to non-military and non-governmental organizations.

MNIS occurs when all authorized partners have timely access to, and can create, transmit, receive, process, and store, the information necessary to perform their assigned multinational mission. Much of the information is sensitive, due to its operational or intelligence value. The MNIS goal is for each U.S. military organization to use its existing information and communication systems to securely share information with authorized multinational partners.

However, not all information can be shared. Some information is more sensitive and, therefore, requires more protection than other information. Similarly, some information is more sensitive to one partner than another. Furthermore, partners do not share all information equally with every partner. The partitioning of information according to access control, need to know, and levels of protection produces categories of information called *information domains*[2] which are discussed in Chapter 2 of this document.

Securely transferring information electronically between information domains is challenging, but no longer can "sneaker nets" be the primary information transfer technique between domains. Today, the risks of sharing information too late—or not sharing information at all—often are greater than the risks associated with sharing the information. This PP helps decision-makers manage their security risks and support the eventual fielding of appropriately secure MNIS solutions.

This Protection Profile focuses on military MNIS requirements. Specifically, this PP discusses sharing command, control, and intelligence information classified no higher than Secret. However, a broader set of military and non-military customers may also recognize their specific situation from this analysis and find the guidance useful.

1.3.1 Operational View[3]

The C/S/As require a multinational information sharing (MNIS) capability to maintain a timely, shared visualization of the battle space with multinational partners. It must provide the ability to plan, coordinate, and conduct military operations using commonly available network components. Information to be shared crosses the three principal elements of the military mission: Operations, Intelligence, and Logistics. Such capability must provide the C/S/As the ability to share this releasable information with their multinational partners while also maintaining confidentiality, integrity, and availability of U.S.-Only[4] networks and unreleased

[1] *Joint Vision 2020*, U.S. Department of Defense, page 4, June 2000 (http://www.dtic.mil/jv2020/).

[2] *Information Assurance Technical Framework,* National Security Agency, Release 3.0, page 1-4, September 2000 (http://www.iatf.net/framework_docs/version-3_0/).

[3] Scenarios that attempt to capture the operational environment are contained in Appendix D.

[4] By "U.S.-Only" we are referring to access by U.S. citizens and by specifically approved foreign personnel who have been granted equivalent authorization as U.S. citizens.

information. Multinational forces must develop, coordinate, and share releasable operations plans, orders, and directives such as a Common Operational Picture (COP), a Common Intelligence Picture (CIP), and Air Tasking Orders. Such reports are based on timely sharing of Operations, Intelligence, and Logistics information that describe the status of multinational forces, the details of intelligence information, the location of hostile forces, and the status of theatre logistics and operations.

1.3.2 Technical View

The following list provides a technical view of the MNIS data exchange requirements derived from Combatant Command-originated messages and documents. It does not attempt to uncover every requirement. Our hope is that the C/S/As will view their specific requirements from within this framework and will apply the principles and techniques discussed to share information with their operational partners as securely as practical.

The data exchanges required between the U.S. and its multinational partners to pursue multinational missions is broad, extending from simple, structured (typically ASCII) data to sophisticated formats including those that enable audio streaming, chatting, and collaboration.

At a minimum, this involves the following data types:

- Simple data files (e.g., text files, formatted data files, COP track data)
- Complex documents (e.g., Microsoft documents)
- Imagery and graphics files
- Audio and video files
- Web documents (e.g., HTML, XML)
- Software application files (e.g., text or binary executables)
- Database files and updates (e.g., COP, CIP)
- Network and system management information

1.3.3 Specific Operational Requirements

Information sharing requirements may be derived and analyzed by first understanding the concept of operations and capabilities needed to support information sharing. These capabilities may be categorized and described in a small number of required operational scenarios. Appendix D, titled “MNIS Operational Scenarios” includes descriptions of the following four operational capabilities that are desired to support effective information sharing:

- Report Composition Utilizing Multiple Information Domains
- Report Distribution to Multiple Information Domains

- Collaboration Among the U.S. and Its Partners
- Automatic Feeds Between Different Information Domains

Analyses of the operational scenarios and customer identified capabilities have resulted in the following summary of specific operational requirements (as applied to the data types identified above) to support all authorized participants contributing to the multinational mission:

1. Transmitting (pushing) and accessing (pulling) data files from one information domain to another. These functions include users transmitting and accessing files to and from operational file servers and web servers.
2. Exchanging information using secure electronic mail.
3. Using special-purpose applications, such as planning tools, collaborative production applications, and command and control applications (e.g., Global Command and Control Systems [GCCS] and the Defense Messaging System [DMS]).
4. Transmitting and receiving tracking data feeds automatically from one information domain to another.
5. Scheduling and coordinating activities using a shared calendar.
6. Collaborating using interactive, real-time tools, such as chat and whiteboards.
7. Providing voice and video teleconferencing.
8. Working in multiple information domains from a single workstation.
9. Using hardware and software components that are releasable to the multinational partners.
10. Managing the functionality and security of the information systems.
11. Establishing and maintaining Communities of Interest (COIs)[5] for data separation.
12. Protecting multinational information and resources, as directed by memoranda of agreement among partner nations.
13. Protecting the U.S.-only information and resources, as directed by U.S. policy and memoranda of agreement among partner nations.

[5] See glossary (Appendix C) for a definition of "Community of Interest." Please note that we differentiate between a COI and bilateral communications. See also section 2.2.4.

1.4 Related Protection Profiles

- *A Goal VPN Protection Profile for Protecting Sensitive Information*, Release 2.0, July 2000
- *Application-level Firewall for Medium Robustness Environments*, Version 1.0, June 2000
- *Department of Defense Mail Guard for High Robustness Environments Protection Profile*, Version 0.1, September 2001
- *Intrusion Detection System Analyzer*, Version 1.1, December 2001
- *Intrusion Detection System Scanner*, Version 1.1, December 2001
- *Intrusion Detection System Sensor*, Version 1.1, December 2001
- *Intrusion Detection System System*, Version 1.4, December 2001
- *Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness*, Version 1.22, May 2001
- *Traffic Filtering Firewall For Medium Robustness*, Version 1.4, May 2000
- *U.S. Department of Defense Firewall Protection Profile for Basic Robustness Environments*, Version 0.6a, September 2001
- *U.S. Department of Defense Virtual Private Network (VPN) Boundary Gateway Protection Profile for Basic Robustness Environments*, Version 0.6, September 2001
- *Virtual Private Network Protection Profile for Protecting Sensitive Information*, Release 1.0, February 2000

1.5 Evaluated Assurance Level Requirement

The MNIS PP differs from most protection profiles because it is written for a system of systems, and not for an individual component or product. Section 2.3 introduces four categories of security functionality (Access Control, Cross-Domain Filtering, Security Administration, and Transmission Security) that are required in the MNIS Target of Evaluation (TOE). As noted in Section 6.4, the minimum Evaluated Assurance Level (EAL) for the categories Access Control and Security Administration is EAL 4 Augmented and the minimum EAL for Cross-Domain Filtering is EAL 5 Augmented. This protection profile does not specify a minimum EAL for Transmission Security. See Section 5.2.4 for details.

The MNIS PP lists the assurance components that are necessary to augment the EAL 4 and EAL 5 levels. Because of the security threats associated with multinational operations, some assurance components for the MNIS TOE are augmented to EAL 6. Even higher assurance may be appropriate in some real-world deployments of a multinational environment based on the MNIS PP, depending on the actual expected threats, the sensitivity of the information, and the risks posed by partnering with certain nations and organizations.

The published arrangement[6] for mutual recognition of Common Criteria certificates applies to CC certificates only at or below EAL 4. Because the EAL for this protection profile exceeds the limit imposed by the "Arrangement" document, the U.S. Department of Defense may choose to deny certificates that are not issued by the U.S. Other participating nations are under no obligation to recognize U.S. certificates with assurance components exceeding EAL 4.

1.6 Conventions

This document is organized based on Annex B of Part 1 of the Common Criteria (CC). There are several deviations in the organization of this profile. First, rather than being a separate section, the application notes have been integrated into the requirements. However, the rationale for the security objectives and requirements are in a separate chapter. Second, the security functional requirements are grouped into four categories of security functionality. These four categories are introduced in Section 2.3.

In the requirement sections, for each subsection that represents a CC requirement family or component, there is a mnemonic in parenthesis. These refer to the requirement section in the CC from which each component was derived. Requirement elements have these references included as superscripted text at the end of the element. In some of the requirements, deviations have been made from the CC text. Each deviation is explained in a footnote on the page where the deviation occurs, rather than collecting all of the explanations as endnotes or in a separate appendix.

[6] *Arrangement on the Mutual Recognition of Common Criteria Certificates in the Field of Information Technology Security*, 5 October 1998. The United States of America is one of the participants in the *Arrangement*.

2 - TOE Description

The MNIS Target of Evaluation (TOE) is defined to include all of the U.S. systems, subsystems, facilities, processes, and procedures for sharing information between the U.S. and its partners. Although each partner is expected to provide comparable systems, subsystems, facilities, processes, and procedures, the MNIS TOE explicitly does not include systems that are not U.S.-controlled. "U.S.-controlled" means physical and administrative control. Control may be delegated to non-U.S. personnel or organizations under certain circumstances. The U.S. and its partners may negotiate implementation agreements based upon this PP, but partner-controlled and multinational-controlled systems are beyond the scope of this PP.

To address the operational requirements itemized in the previous chapter and explain the Target of Evaluation that is the subject of this PP, this chapter will:

- Introduce the concept of "**Information Domains**" (Section 2.1),
- Discuss how the users' requirements to transmit and access information within and between these information domains may be implemented in a more physically oriented "**MNIS Model**" (Section 2.2),
- Propose an "**MNIS High-Level Security Architecture**" which will be an overlay on top of the TOE portion of the MNIS Model (Section 2.3).

2.1 Information Domains

An "*information domain*" is the virtual space in which all the contained information is classified at a ***single*** level and all personnel with physical or electronic access to that information are appropriately cleared and authorized to that level of information and resources. Need-to-know handling restrictions, data separation, and controlled access based on authenticated user identification and verified authorization occur within an information domain. These mechanisms are also appropriate for physical environments that will be discussed in a subsequent section.

In order to discuss MNIS operational requirements it is helpful to have in mind a high-level concept of the information involved. We attempt to provide this high-level view in Figure 1 by representing the segregation of information into multiple information domains**.** We do this to describe the controlled sharing that must exist in a classified, military system configuration. In this figure, we are not describing physical entities. Instead, it represents a U.S.-centric view of how information is generated and used in a restricted **U.S.-Only Information Domain**, reviewed for release to a **MNIS Information Domain**, and shared with multinational partners' **Partner National Information Domain(s)**. The following four subsections describe these three information domains and the class of sub-domains within the MNIS Information Domain that are shown in Figure 1.

2.1.1 U.S.-Only Information Domain

This domain represents an information domain that contains U.S. Secret information restricted from distribution to non-U.S. citizens and unauthorized U.S. citizens. The physical implementation of this information domain equates to one or more environments consisting of authorized U.S. citizens, computers, software, networks and security devices that may be organized in a variety of ways but all be under the direct control and administration of the U.S.

2.1.2 MNIS Information Domain

This domain represents the information domain that contains multinational Secret information (downgraded and released information from the information domains of both the U.S.-only domain and the multinational partner domains). The physical implementation of this information domain equates to one or more environments consisting of people from both the U.S. and potentially all partner nations, computers, software, networks and security devices, all of which help compute and organize sharable information.

2.1.3 Partner National Information Domain(s)

These represent multiple foreign partner information domains. These domains contain foreign partner originated information that is not releasable outside of the country of origin without further review. In the case of nation *a*, say Australia, Partner National Domain C_a typically contains Australia-Only information. We assume that Australia (or any other partner) reviews information prior to releasing it to the MNIS Domain. In some cases, Partner National Domain C_n represents the information domain of another type of organization. For example, Partner National Domain C_n could represent a non-DoD, U.S. agency tasked to support the multinational effort. In a physical implementation, Partner National Domain C_n equates to Partner Nation *n*'s national Secret network (one or more environments) that is equipped with that nation's supplied computers, software, networks, system administration and security mechanisms, and manned by nation *n*'s personnel and administrators.

2.1.4 Communities of Interest (COIs) Information Sub-Domains

COI sub-domains are supported within the MNIS Domain. These COI sub-domains contain MNIS Secret information (downgraded and released information from the information domains of both the U.S.-only domain and the other Partner National Domains) which have the additional handling restrictions to provide "need to know" data separation. In Figure 1, they are depicted as intersecting circles within the MNIS Domain. Data separation within this domain for these types of COIs use security mechanisms that are less robust, typically described as privacy mechanisms, to enforce the separation as opposed to more robust confidentiality separation. Medium robustness separation mechanisms are sufficient to separate COI information within the MNIS Information Domain.

Throughout the remainder of the PP the specified capabilities of the TOE will address the information flows and sharing that take place ***within*** the MNIS Domain, as well as the

information flows and interfaces ***between*** the MNIS Domain and either the U.S.-Only Domain or the various Partner National Domains.

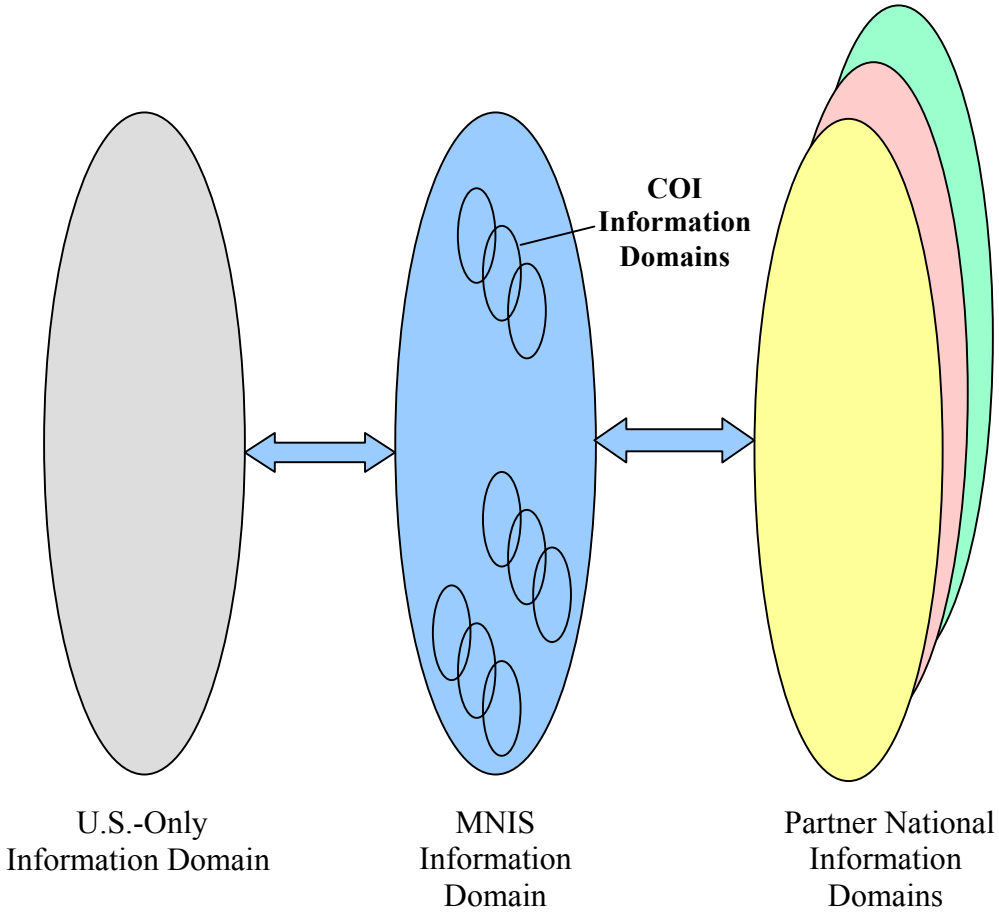


Figure 1 - Multinational Information Sharing (MNIS) Domain View

2.2 MNIS Model

This section of the PP introduces the concept of a more physical view of the MNIS TOE by defining a MNIS Model (to be referred to as the "Model"). The Model will help with the derivation and specification of appropriate and adequate security requirements for the TOE and TSE (TOE Security Environment) associated with the "controlled sharing" of information between the information domains defined in the previous section. It will serve as the basis for the development and further analysis of the proposed MNIS High-Level Security Architecture to be discussed in subsequent sections.

The Model description will describe various characteristics and attributes of the TOE and will allow for components of the TOE to be distributed among various physical "***environments***." In

this context the term "*environment*" refers to an "aggregate of procedures, conditions, and objects affecting the development, operation, and maintenance"[7] of an information system. In terms of the TOE, these are mostly physical aspects such as geographic location, physical security, and clearances of personnel with physical access.

The MNIS Model pictured in Figure 2 includes three categories of environments, the U.S.-Only Environment(s), the Multinational Information Sharing Environment, and the Partner National Environment(s).

In addition to characterizing these physical environments, the Model description will include an explanation of allowed and unauthorized **data flows** between these environments.

2.2.1 Purpose of the MNIS Model

In subsequent sections of the PP, the team uses the Model (Figure 2) to define appropriate threats, assumptions, security policy, and security objectives applicable to the TOE. Then, the team derived applicable security functional and assurance requirements for the TOE.

In the context of the definition of the Model, the TOE will include various functional components that are controlled and administered by U.S. personnel, and contained within the MNIS and U.S.-Only environments. These components will process information that is restricted to the MNIS Information Domain and, depending on actual location, will be physically accessible by either U.S.-Only or U.S. and partner personnel.

With an understanding of the Model, customers and their supporting System Security Engineering (SSE) teams will be able to:

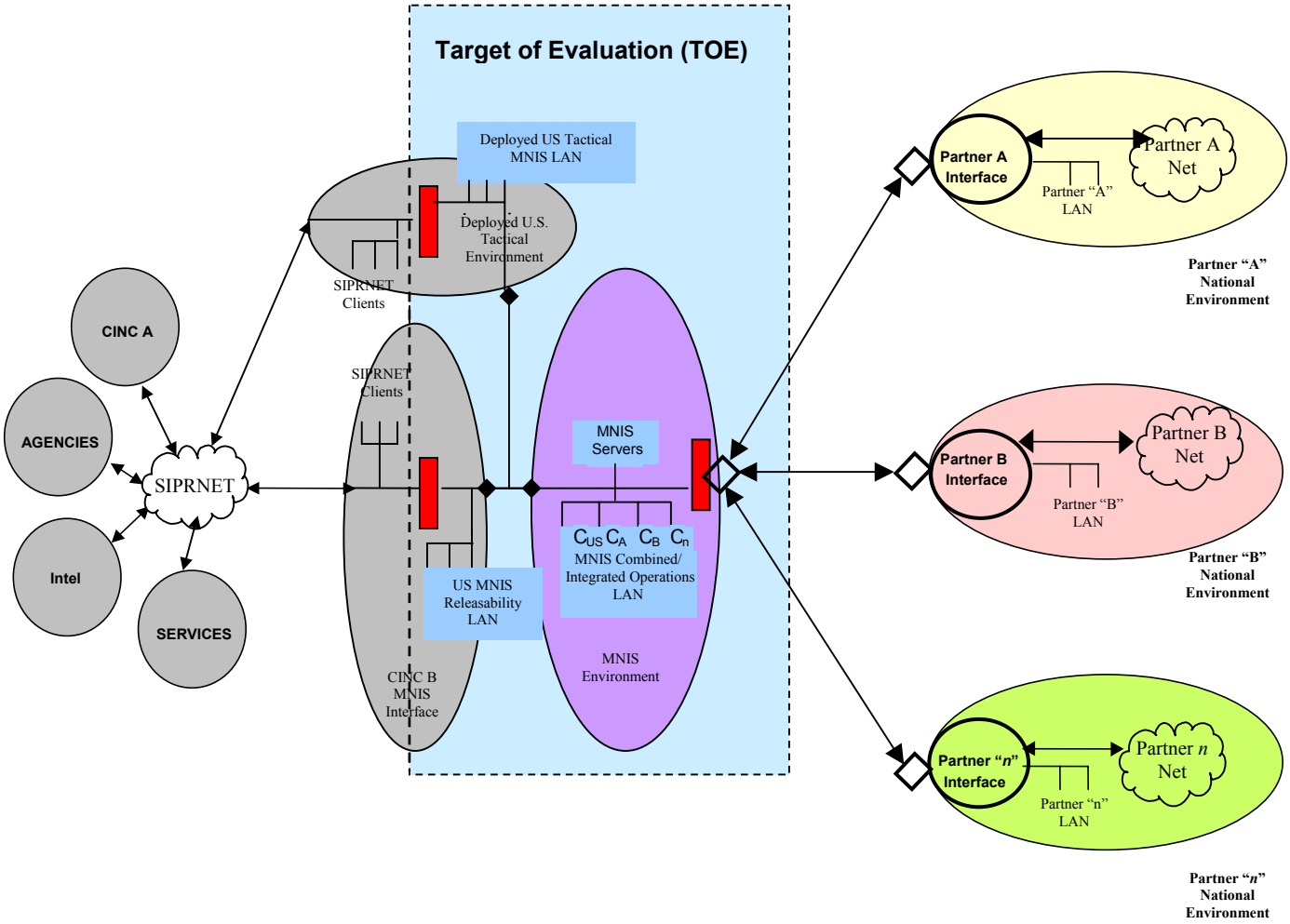
- Identify their specific requirements from the generic example presented in the Model;
- Concur with the PP team's analysis that the security functional and assurance requirements specified for the TOE are appropriate to securely share information among their partners; and,
- Design and implement a specific solution composed of available security products and protocols that will provide an equivalent capability as attributed to the Model (to include both the TOE and TSE).

2.2.2 High Level Premises Concerning the MNIS Model

As a first step in developing the Model, the PP team formulated the following general premises concerning the Model:

[7] Source: *National Information Systems Security Glossary*, NSTISSI No.4009, National Security Agency, September 2000.

- **Unlabeled data must be reviewed prior to release from one information domain to another.** Unlabeled data that has either been created on, stored in, or transmitted over, a system-high network must be subjected to review before it can be re-graded and/or released to individuals or processes which are not authorized at the originally assumed classification and/or compartmentation.
- **The author of information is the appropriate person to assert the initial classification of the information.** However, when information (or some subset) is to be shared with individuals outside of the originator's information domain and is subject to re-grading and/or release, a professional release authority, such as a Foreign Disclosure Officer, must assure the originator-asserted classification is appropriate and the re-grading is performed in accordance with policy.
- **Information released to the MNIS Information Domain is, in general, available to all partners with the only exception being COI data segregation.** Generally, information released by the U.S. into the MNIS Information Domain is releasable to all partners. However, COIs provide "need-to-know" data separation within the MNIS Domain. Medium robustness mechanisms are used to maintain COI data separation.
- **MNIS partnership agreements and supporting systems must be adaptable and frequently assessed.** Partnerships that require multinational sharing of information are very hard to quantify. They can be of a very short duration or long standing. Their supporting IT infrastructures may potentially include products with which the U.S. is familiar and comfortable as well as commercial or foreign developed products, of which the U.S. has little knowledge. All multinational partners must comply with the interface requirements that enable communication with the MNIS Information Domain.
- **Applications and connectivity between partners within the MNIS Information Domain should be feature rich and as robust as possible to enable seamless interoperability and information sharing**.
- **Availability and the capability of applications and connectivity between the MNIS Information Domain and other U.S. and foreign information domains may need to be restricted to ensure the security and integrity of unreleased data.**
- **In general, IT products and processes located within the U.S.-Only and the MNIS environments will be authorized and administered by U.S. personnel or their designated representatives.** Each partner is responsible for its own national IT environment.



	U.S.-Only Environments
	Multinational Information Sharing (MNIS) Environment (U.S. Controlled)
	Partner "A" Environment
	Partner "B" Environment
	Partner "n" Environment

	CINC B MNIS Interface
	MNIS Information Domain
	In-Line Encryptor
	Exportable In-Line Encryptor
	TOE Boundary

Figure 2 - Multinational Information Sharing (MNIS) Model

2.2.3 Elements of the Model

As previously stated, the Model is composed of various physical ***"environments"*** that are interconnected by uniquely defined ***data flows*** and interfaces. These environments include U.S.-Only environments, a MNIS Environment, and Partner National environments. In later sections of this PP, the description of the Model's environments and data flows will be used to analyze applicable threats and policies, derive appropriate security objectives, and functional and assurance requirements for the Target of Evaluation (TOE) and for interfaces between the TOE and other information domains.

2.2.3.1 MNIS Model Physical Environments

2.2.3.1.1 U.S.-Only Environment(s) Characteristics

Though Figure 2 depicts the U.S.-Only Environment (including the U.S. MNIS Releasability LAN, to be referred to as the "Releasability LAN") as a single environment, the intent is to represent only a possible configuration. Other configurations are possible and may be implemented in a distributed fashion with an interface physically located at each Combatant Command or deployed tactical environment. The following characteristics apply to the U.S.-Only Environment:

1. The SIPRNET is the primary protected backbone, wide-area network (WAN) interconnecting Secret, U.S.-Only environments.
2. SIPRNET policy limits unrestricted access and connectivity to the WAN to only fully cleared U.S. citizens.
3. SIPRNET is a Secret, U.S.-Only, system-high network and consequently all data that is generated, stored, or transmitted on the SIPRNET, is considered Secret, U.S.-Only, contained within the Secret, U.S.-Only Information Domain, and procedurally marked accordingly.
4. All IT resources that are included in the U.S.-Only environments (and consequently within the SIPRNET) are authorized, administered, and maintained by U.S. authorities and their designated representatives.
5. Within U.S.-Only environments, boundary protection mechanisms may be included to allow safe connectivity to differing information domains (to include the MNIS Information Domain).
6. By including appropriate boundary protection mechanisms within the U.S.-Only Environment, provisions may be made to physically and/or logically partition the environment into two separate information domains; i.e., instantiate both a U.S.-Only LAN and a Releasability LAN within the U.S.-Only Information Domain. To accomplish effective data separation within the U.S.-Only Information Domain trust technology or periods processing may be employed.

7. U.S.-Only environments may be either strategic (i.e., Combatant Command strategic interfaces) or tactical, deployed physical environments.
8. The Releasability LAN will be the primary *localized* networking resource utilized by Combatant Command-assigned (or U.S. tactical forces) personnel who have a requirement to share information with foreign partners. By *localized*, it is implied that the Releasability LAN will typically be located within the physical boundary of a U.S.-Only Environment.
9. Personnel access to the Releasability LAN portion of the U.S.-Only Environment will include both appropriately cleared (Secret or higher) U.S. citizens as well as specified foreign allies who have been assigned to designated U.S. positions within the U.S. Command structure. These integrated foreign personnel are granted privileges equivalent to fully cleared U.S. personnel for access to data and resources within their assigned Area of Responsibility. Though U.S. personnel and integrated foreign personnel are cleared for access to Secret data, they must also have authorization for access to the specific mission releasable data.
10. Data transmitted or stored within the Releasability LAN portion of the U.S.-Only Environment *may be* marked to designate the country of origin (optional) and *must* be marked[8] to designate its classification (e.g., "Secret"), mission name (e.g., "Desert Storm"), and releasability authorization (e.g., REL. U.S., U.K.).

Example: "U.S.-Secret, Desert Storm, REL. U.S., U.K.".

2.2.3.1.2 Multinational Information Sharing (MNIS) Environment Characteristics

The concept of combined or integrated operations is modeled as the depicted MNIS Environment. Within this environment, U.S. and foreign partners are working shoulder-to-shoulder in a combined operation that is focused on a common mission with specific objectives. This environment will include users who are typically either physically collocated or at least within close proximity and under the direct control of a designated Command Authority. Usually, this Command Authority is a U.S. Combatant Commander but may be any partner nation Commander. Normally, the IT systems within this environment will be provided and administered by the U.S. However, in some situations, administrative control of this environment may be relinquished to explicitly designated operational partners who perform their duties in accordance with a mutual agreement. The following characteristics apply to the MNIS Environment:

[8] This is an example of a technique for labeling data. It is not intended to be a proposed labeling "standard." The intent is to identify necessary information that must be conveyed by such a standard.

1. Personnel access to the MNIS Environment (and data stored or transmitted within it) will include both Secret cleared U.S. citizens as well as specified foreign partners who have been designated as MNIS users and granted equivalent access and authorization. MNIS partner nation personnel located within the MNIS Environment are administratively reportable to a single Command Authority that may be either a U.S. or foreign partner commander. The MNIS users are focused on a common mission with specific objectives. Once those objectives are achieved or superceded, the combined operation is typically terminated.
2. The MNIS Environment will contain information that has been determined releasable by the partner nations that originated it, and contained within the MNIS Information Domain.
3. All information contained within the entire MNIS Domain is replicated as necessary, and available within both the MNIS Environment and the Releasability LAN portion of applicable U.S.-Only environments.
4. Information contained within the MNIS Environment may be further segregated into COI information sub-domains that limit the distribution of information to various sub-sets of the partners assigned to the particular multinational mission(s) conducted within the MNIS Environment.
5. All IT resources that are included in the MNIS Environment are authorized, administered, and maintained by U.S. authorities and their designated representatives.
6. Data transmitted or stored within the MNIS Environment *may be* marked to designate the country of origin (optional) and *must* be marked to designate its classification (e.g., "Secret"), mission name (e.g., "Desert Storm"), and releasability authorization (e.g., U.S., U.K.).

Example: "U.S.-Secret, Desert Storm, REL. U.S., U.K."

2.2.3.1.3 Partner National Environment(s) Characteristics

The Partner National Environments represent distinct environments where that country's national operations are conducted. These environments also include interfaces to the MNIS Environment (unless the partner declines to interconnect to the MNIS Environment). Frequently, the U.S. will provide the MNIS interfaces included within these environments. However, when these interfaces are provided by the partner nation, they may be required to meet a minimal standard that the U.S. (or its designated representative) will define for multinational operations. The following characteristics apply to the Partner Environments:

1. The Partner National Environments include protected networks similar to the U.S. SIPRNET on which they conduct classified national operations. Our foreign partners

will require access to their own internal information as well as information which they have determined is releasable or is developed as part of multinational operations in which they are involved.

2. Foreign national interests and supporting policy limit unrestricted access and connectivity to the Partner National Environment and their national network to only fully cleared citizens of their nation.
3. Foreign partner's classified networks operate in a national Secret system-high mode and consequently all data that is generated, stored, or transmitted on these networks, is considered Secret, Nation "*x*", and marked in accordance with their national policy[9].
4. All IT resources which are included in the Partner National Environments are authorized, administered and maintained by their own national authorities and their designated representatives.

2.2.3.2 Data Flows

This portion of the protection profile describes the various data flows that occur in the model. Referring back to Figure 1, three principal categories of data flows are apparent. One occurs between the U.S.-Only Information Domain and the MNIS Information Domain. The second occurs internal to the MNIS Information Domain (including COI data flows). The third occurs between the MNIS Information Domain and the Partner National Environments.

The following subsections provide a high-level description of each category of data flow. The intent is to introduce uniform terminology that will be used in later sections of the PP to examine and document the risks and countermeasures associated with these data flows. For the purposes of this PP, the following terminology is used to describe data flows.

PUSH - a user transfers a file to a destination computer.

PULL - a user views a directory of files on a remote computer or server and extracts information that is transferred to his computer.

E-MAIL - a user sends information to one or more users. (This user-initiated form of Push is described separately to highlight some differences that may impact security considerations; for example, the user may wish to attach files[10] to the email.)

[9] Partner national information marking standards must be understood and consistently interpreted by all MNIS partners within the MNIS Information Domain in accordance with a negotiated and agreed upon MNIS security policy.

[10] For a discussion of files attached to electronic mail, see also *Department of Defense Mail Guard for High Robustness Environments Protection Profile*, Version 0.1, 30 September 2001

AUTOMATIC FEED[11] - files or a continuous flow of data are automatically transferred from one server to another server, based on pre-arranged rules, configuration settings, and formats. (This process-initiated form of Push is described separately to highlight some differences that may impact security considerations.)

REQUEST - a requesting user transfers a question, query, or form to another user or process under the control of the recipient or process. The requesting user expects a subsequent action from the recipient or process.

COLLABORATION[12] - two or more users confer with each other or supporting processes (typically synchronously).

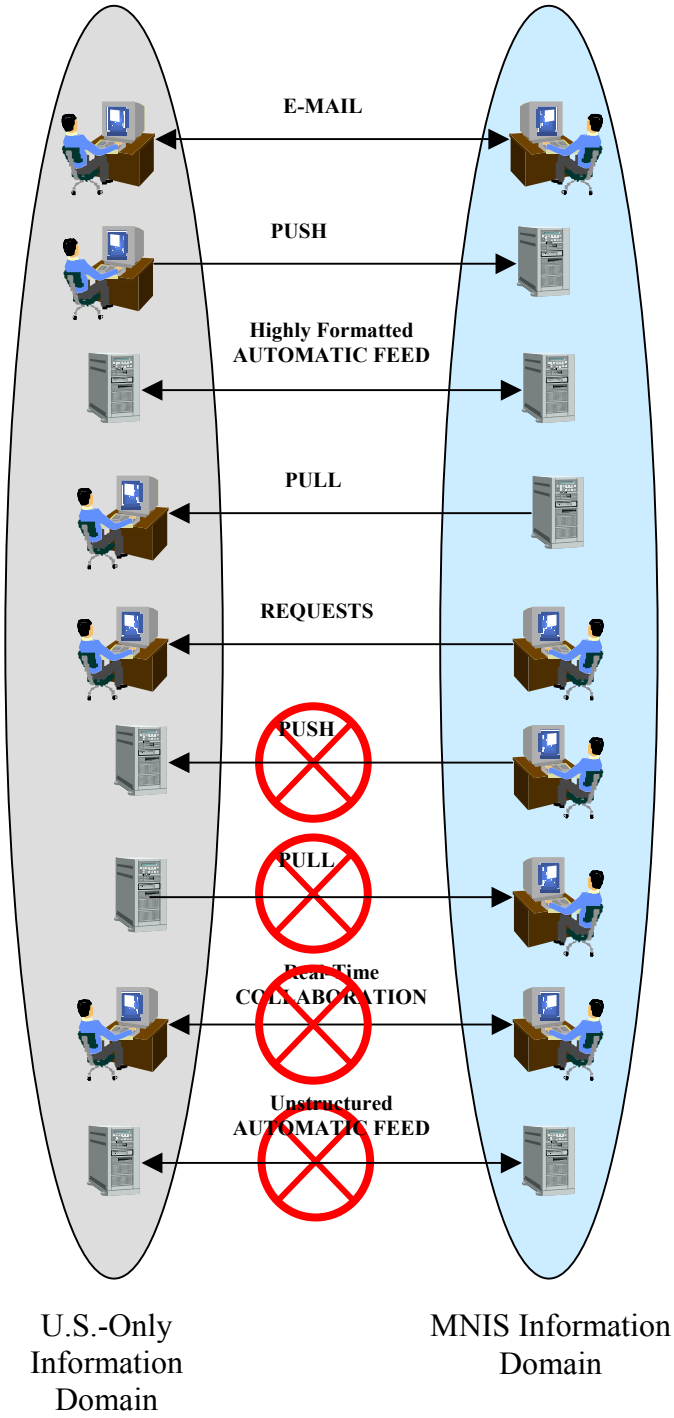
These subsections indicate a few of the security considerations related with these flows. However, the complete technical details and security risks associated with each of these types of data flow are discussed in later sections of this PP.

2.2.3.2.1 Data Flows ***between*** U.S.-Only Information Domain *and* MNIS Information Domain

The enumerated operational requirements imply the need for information to flow between U.S-Only Information Domain (including U.S.-Only SIPRNET Clients) and the MNIS Information Domain (including the physically co-located Releasability LAN). There may be restrictions placed on these data flows that result from the necessity to ensure the confidentiality, integrity and availability of the U.S.-Only Information Domain, associated data and network resources. These restrictions may potentially limit the applications and protocols that will be allowed to exchange information across this data path. Consequently, capabilities between these domains may be less robust and perhaps not as application rich as either desired or incorporated within the confines of the MNIS Environment. The U.S-Only to MNIS Information Domain interface will include the data flows as pictured in Figure 3 and discussed in subsequent sections.

[11] See Appendix D Scenario 4.

[12] See Appendix D Scenario 3.



E-Mail transfer between users in U.S-Only and MNIS domains.

U.S. User initiated **PUSH** to MNIS domain (e.g., FTP POST)

Highly Formatted Automatic FEED between U.S.-Only and MNIS domains based on pre-arranged policy and pre-configured formats (i.e., subscription service, report distribution, highly formatted data feed)

U.S. Users **PULL** from MNIS domain (e.g., FTP GET)

MNIS User initiated **REQUEST** to U.S. User (e.g., MNIS query, subscription request, data PULL from MNIS request)

Un-coordinated data **PUSH** is prohibited (e.g., FTP POST initiated by MNIS Users)

Un-coordinated data **PULL** is prohibited (e.g., FTP GET initiated by MNIS Users)

Real-Time **Collaboration** between U.S and MNIS Users is prohibited

Unstructured Automatic FEED between U.S.-Only and MNIS domains is prohibited.

Figure 3 - Data Flows between U.S.-Only and MNIS Information Domains

2.2.3.2.1.1 U.S.-Only Information Domain **Export** Data Flows

The following data flows require review to ensure the information is authorized for release to foreign national partners (e.g., re-grade the data to effectively remove U.S.-Only restrictions). In addition, the review must include a determination as to which multinational relationship/mission and specifically which multinational partners the data will be releasable to, and that the data is marked accordingly (e.g., Secret/ Desert Storm/REL. U.S./UK).

Typical techniques to be considered when crafting a solution for these sorts of export data flows include content filtering and restricting data to structured and/or strictly defined data formats.

- E-Mail transmission out of the U.S.-Only Information Domain for delivery to MNIS Users.
- Data Push from U.S.-Only Information Domain to a server in the MNIS Information Domain (i.e., co-located Releasability LAN) may be prompted by these actions:
  1. U.S. users located in the U.S.-Only Information Domain initiates a data Push, and
  2. U.S. User responds to a MNIS User Request to Push data to the MNIS Information Domain.
- Highly Formatted Automatic Feed[13] between U.S.-Only and MNIS domain servers based on pre-arranged policy and pre-configured data formats (i.e., specifically defined subscription service response, configured report distribution, or highly formatted data base feeds).

Optionally, either by policy and/or by the determination of the data author, the exported data may also be marked to indicate country of origin (e.g., U.S. Secret/Desert Storm/REL.US/UK).

Additional security services that may be considered for these data flow types may include non-repudiation of origin, data integrity, confidentiality/privacy protection, and authentication. Audit recording should also be considered for each occurrence of these data exports.

2.2.3.2.1.2 U.S.-Only Information Domain **Import** Flows (i.e., Low-to-High Pull)

The following data flow must be reviewed to ensure that imported data does not include malicious code that could jeopardize the integrity, availability, or confidentiality of critical U.S.-Only data maintained within the U.S.-Only Information Domain. All data imported from the MNIS Information Domain will be integrity protected to ensure that it has not been modified by unauthorized entities (non-multinational partners). In addition, data imported into the U.S.-Only

[13] See Appendix D Scenario 4 for a description of Highly Formatted Automatic Feed.

Information Domain must have originated from and be destined for delivery to only properly identified, authenticated and authorized recipients and processes in accordance with distribution restrictions incorporated in the multinational data labels. Additional security services that may be considered for these data flow types may include non-repudiation of origin. Audit recording should also be considered for each occurrence of these data imports.

- E-Mail transmission out of the MNIS Information Domain for delivery to U.S. Users located within the U.S.-Only Information Domain.
- Data Pull into the U.S.-Only Information Domain initiated by U.S. users located within the U.S.-Only Information Domain.
- Requests originated by users located within the MNIS Information Domain, directed to specific data owners located within the U.S.-Only Information Domain which request one of the following subsequent actions:

    1. Data Push from the U.S.-Only Information Domain into the MNIS Information Domain, and
    2. Data Pull into the U.S.-Only Information Domain.

- Highly Formatted Automatic Feed[14] between MNIS and U.S.-Only information domain servers based on pre-arranged policy and pre-configured data formats (i.e., specifically defined subscription service response, configured report distribution, or highly formatted data base feeds).

2.2.3.2.1.3 Prohibited or Not-Required Data Flows

The following data flows have been determined to be either unnecessary or to impose excessive risk to the U.S.-Only Information Domain to be included in the capability of the Model:

- Unauthorized data Push into the U.S.-Only Information Domain that has not been previously coordinated with a specific U.S.-Only Information Domain User or from unauthenticated/unauthorized users is prohibited. However, MNIS Users may Request a data Pull into the U.S.-Only Information Domain.
- Data Pull out of the U.S.-Only Information Domain is prohibited. However, MNIS Users may Request a data Push from the U.S.-Only Information Domain.
- Real-Time Collaborative[15] data protocols (e.g., video teleconferencing, Voice over IP, unstructured automatic feeds) are prohibited. However, asynchronous collaboration is not prohibited.

[14] See Appendix D Scenario 4.

[15] See Appendix D Scenario 3 for description of Collaboration.

- Unstructured Automatic Feeds[16] between U.S and MNIS information domains are prohibited.

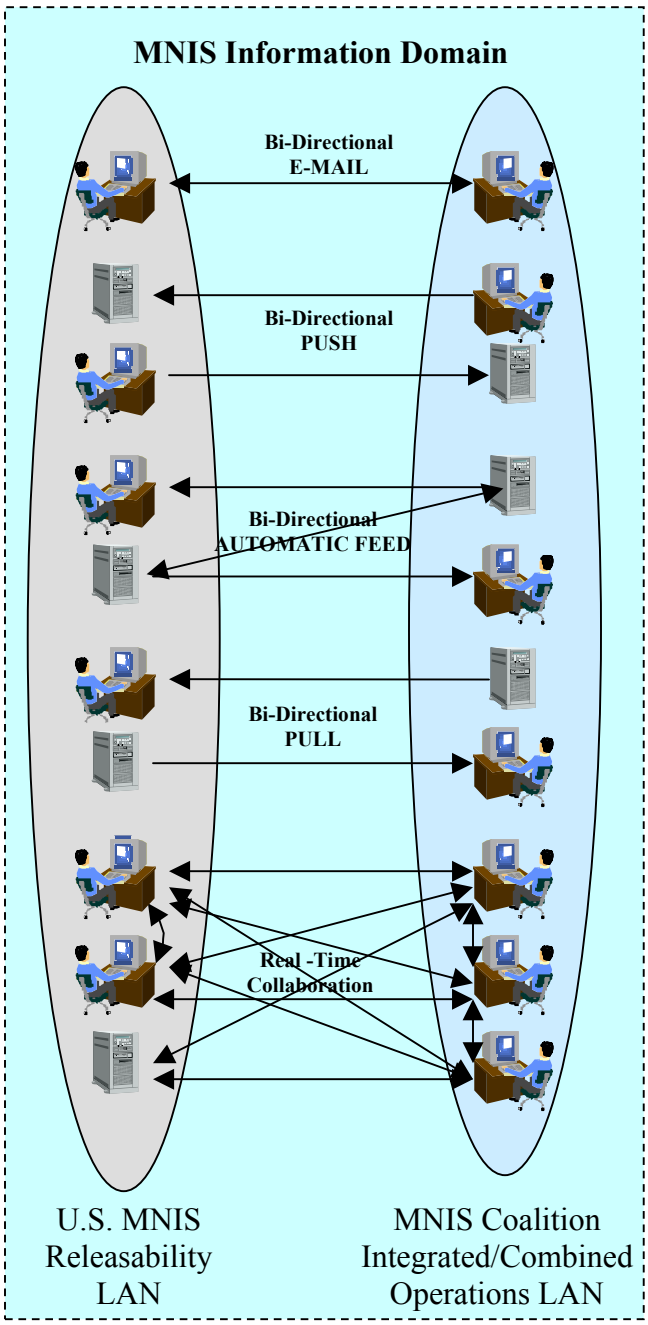
2.2.3.2.2 Data Flows ***internal*** to the MNIS Information Domain

As shown in Figure 4, the MNIS Information Domain may be distributed across multiple environments with elements in the U.S.-Only Environment (the Releasability LAN) and elements in the MNIS Environment (MNIS Combined/Integrated Operations LAN). A physically dispersed information domain is significant because elements of the same information domain may have to comply with different physical security constraints, security policy, or operational doctrine associated with the physical environment which contains the elements.

One of the main purposes in viewing the MNIS Environment as composed of physically dispersed elements is to allow for the possibility of strategic and deployed elements of the MNIS Information Domain having a broad variety of popular protocols and applications with which to communicate. Users with access to the strategic Releasability LAN or the deployed MNIS Combined/Integrated Operations LAN may use a rich set of applications to perform their information sharing mission among all of their multinational partners without the need for narrowly defined filtering, data segregation, or high assurance security techniques inhibiting the data flows. The Model's assumptions regarding data flows internal to the MNIS Information Domain are as follows:

- Information re-grading, labeling and release review operations have been performed prior to releasing information to the MNIS Information Domain and are unnecessary for internal MNIS Information Domain data flows.
- Multinational partners have the opportunity to incorporate protective boundary protection at each of their interfaces in accordance with their own national policies.
- Within the MNIS Information Domain, medium robustness data separation and access controls are acceptable to support COI data segregation.
- Within and between the physically dispersed elements of the MNIS Information Domain resources, information and data flows will be protected by whatever security services are required (e.g., confidentiality, integrity, availability, and access control) as dictated by the unique threat environment associated with each physical environment and transmission path.

[16] See Appendix D Scenario 4 for definition of Unstructured Automatic Feed



Bi-Directional E-Mail transfer between internal MNIS domain Users.

Bi-Directional PUSH of data to servers within MNIS domain (e.g., FTP POST)

Bi-Directional Automatic FEED (both Highly Formatted and Unstructured Automatic Feeds) of data between MNIS Users and MNIS servers within the MNIS domain based on pre-arranged policy and pre-configured formats (i.e., subscription service, report distribution, continuous data feed)

MNIS Users **Bi-Directional PULL** data from servers in multiple environments within the MNIS domain (e.g. FTP GET)

Real-time Collaboration between MNIS Users within the MNIS domain

Figure 4 - Internal MNIS Information Domain Data Flows

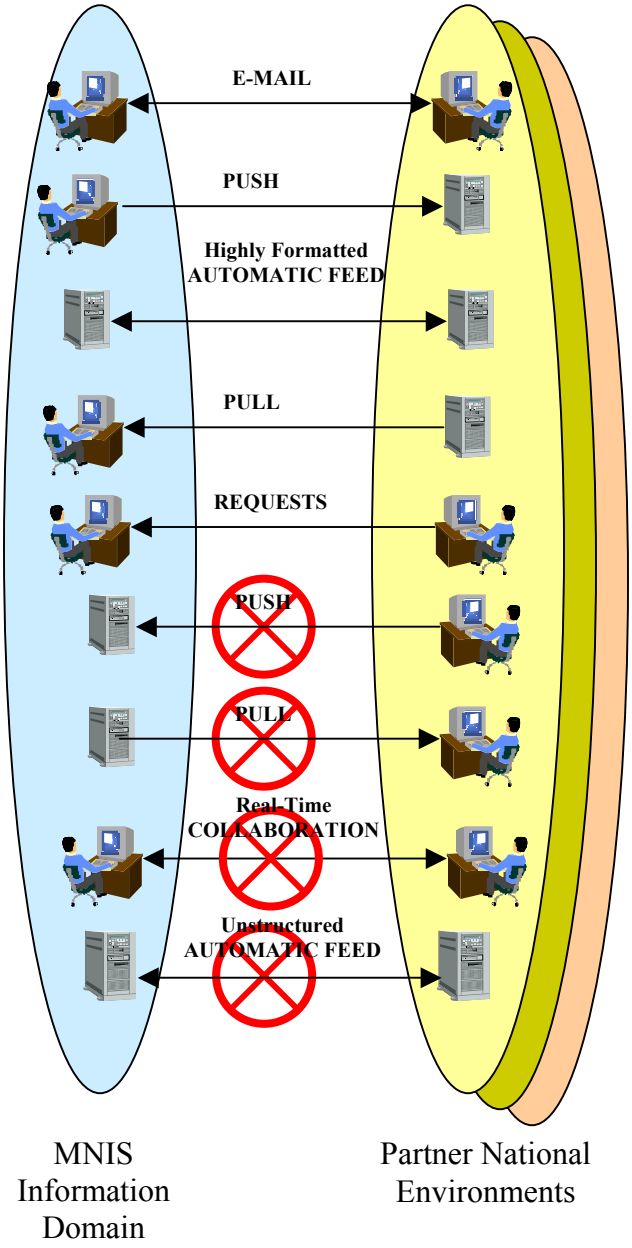
As shown in Figure 4, the following data flows will be allowed within the MNIS Information Domain that includes the Releasability LAN and the MNIS Coalition Integrated/Operations LAN:

- Bi-directional E-Mail transmission between MNIS Users regardless of point of service (i.e., local subscriber service provided either by the Releasability LAN or MNIS Coalition Integrated/Combined LAN).
- Bi-directional data Push and Pull between MNIS Users regardless of point of service (i.e., local subscriber service provided either by the Releasability LAN or MNIS Coalition Integrated/Combined LAN).
- Bi-directional Automatic Feed between users and servers within the MNIS Information Domain (including between distributed elements of the information domain) for the purpose of supporting various automated services such as internal subscription service, configured report distribution, and maintenance of data bases.
- Data flows supporting real-time Collaborative data protocols (e.g., video teleconferencing, Voice over IP, unstructured automatic feeds) between MNIS Users.

2.2.3.2.3 Data Flows ***between*** MNIS Environment *and* Partner National Environments

The enumerated operational requirements imply the need for information to flow between Partner National Environments and the MNIS Environment. There may be restrictions (i.e., MNIS security policy enforcement) placed on these data flows that result from the necessity to ensure the confidentiality, integrity, and availability of the MNIS environment, associated data and network resources. In addition to MNIS policy, these data flows may incorporate additional restrictions to enforce partner nation established rules relevant for controlled sharing of information with their national partners. These restrictions may potentially limit the applications and protocols that will be allowed to exchange information across this data path. Consequently, capabilities within these environments may be less robust and perhaps not as application rich as either desired or incorporated within the confines of the MNIS Environment.

Figure 5 depicts data flows and restrictions that will be enforced between the MNIS Environment and the Partner National Environments as explained in subsequent sections.



E-Mail transfer between users in MNIS Environment and Partner Environments.

MNIS User initiated **PUSH** to Partner Environments (e.g., FTP POST)

Highly Formatted Automatic FEED between Partner Environments and MNIS Information Domains based on pre-arranged policy and pre-configured formats (i.e., subscription service, report distribution, continuous data feed)

MNIS Users **PULL** from Partner Environments (e.g., FTP GET)

Users within Partner Environments initiated **REQUEST** to MNIS User (e.g., data availability notification, data PUSH from MNIS Environment request)

Un-coordinated data **PUSH** (e.g., FTP POST initiated by MNIS Users) is prohibited

Un-coordinated data **PULL** (e.g., FTP GET initiated by MNIS Users) is prohibited

Real-Time Collaboration between Partner Environments and MNIS Information Domains is prohibited.

Unstructured Automatic FEED between U.S.-Only and MNIS domains is prohibited.

Figure 5 - Data Flows between MNIS Information Domain and Partner National Environments

2.2.3.2.3.1 MNIS Environment **IMPORT** from Partner National Environment Data Flows

Partner data that flows into the MNIS Environment must be reviewed to ensure that it does not include malicious code that could jeopardize the integrity, availability, or confidentiality of critical multinational data. Additional security services that may be considered for these data flow types may include non-repudiation of origin. Audit recording should also be considered for each occurrence of these data imports. Typical techniques to be considered when crafting a solution for these sorts of import data flows include content filtering and restricting data to structured and/or strictly defined data formats.

- E-Mail transmission out of Partner National Environments for delivery to MNIS Users located within the MNIS Information Domain.
- Data Pull into the MNIS Information Domain initiated by MNIS Users located within the MNIS Information Domain.
- Requests originated by users located within the Partner National Environments directed to specific data owners located within the MNIS Information Domain which request the following subsequent actions:

  1. Data Push from the MNIS Information Domain into the Partner National Environments, and
  2. Data Pull into the MNIS Information Domain.
- Highly Formatted Automatic Feed[17] between servers located in the MNIS Information Domain and the Partner National environments based on pre-arranged policy and pre-configured data formats (i.e., specifically defined subscription service response, configured report distribution, or highly formatted data base feeds).

2.2.3.2.3.2 MNIS Environment **EXPORT** to Partner National Environment Data Flows

All data exported from the MNIS Environments will be released to only properly identified and authenticated recipients in Partner National Environments who match the mission identification and releasability fields incorporated in the multinational data labels. Typical data labeling will include the following data fields: classification field: Secret, multinational mission identification field: (e.g., Desert Storm), Releasability field: (e.g., nations "A to *n*"). Optionally, either by multinational policy and/or by the determination of the data author, the released data may also be marked to indicate country of origin (e.g., nations "A to *n*").

[17] See Appendix D Scenario 4.

Additional security services that may be considered for these data flow types may include non-repudiation of origin, confidentiality/privacy protection, and authentication. Audit recording should also be considered for each occurrence of these data exports.

- E-Mail transmission out of the MNIS Information Domain for delivery to users located in Partner National Environments.
- Data Push from the MNIS Information Domain may be prompted by these actions:
  1. MNIS Users located in the MNIS Information Domain initiates a data Push, and
  2. MNIS User responds to a partner Request to Push data to the Partner National Information Domain.
- Highly Formatted Automatic Feed[18] between servers located in the MNIS Information Domain and the Partner National environments based on pre-arranged policy and pre-configured data formats (i.e., specifically defined subscription service response, configured report distribution, or highly formatted data base feeds).

2.2.3.2.3.3 Prohibited or Not-Required Data Flows

The following data flows have been determined to be either unnecessary or to impose excessive risk to the MNIS Information Domain to be included in the capability of the Model:

- Unauthorized data Push into the MNIS Information Domain that has not been previously coordinated with a specific MNIS Information Domain User or from unauthenticated/unauthorized users is prohibited. However, partners may Request a data Pull into the MNIS Information Domain.
- Data Pull out of the MNIS Information Domain is prohibited. However, partners may Request a data Push from the MNIS Information Domain.
- Real-Time Collaborative data protocols (e.g., video teleconferencing, Voice over IP, unstructured automatic feeds) are prohibited. However, asynchronous collaboration is not prohibited.
- Unstructured Automatic Feeds between MNIS Information Domain and Partner National Environments are prohibited.

2.2.4 Bilateral Communications Paths Supporting the MNIS Model

Although the MNIS model supports communities of interest (COIs) within the MNIS information domain, the model is not designed to support bilateral communication between the U.S. and partner environments.

[18] See Appendix D Scenario 4.

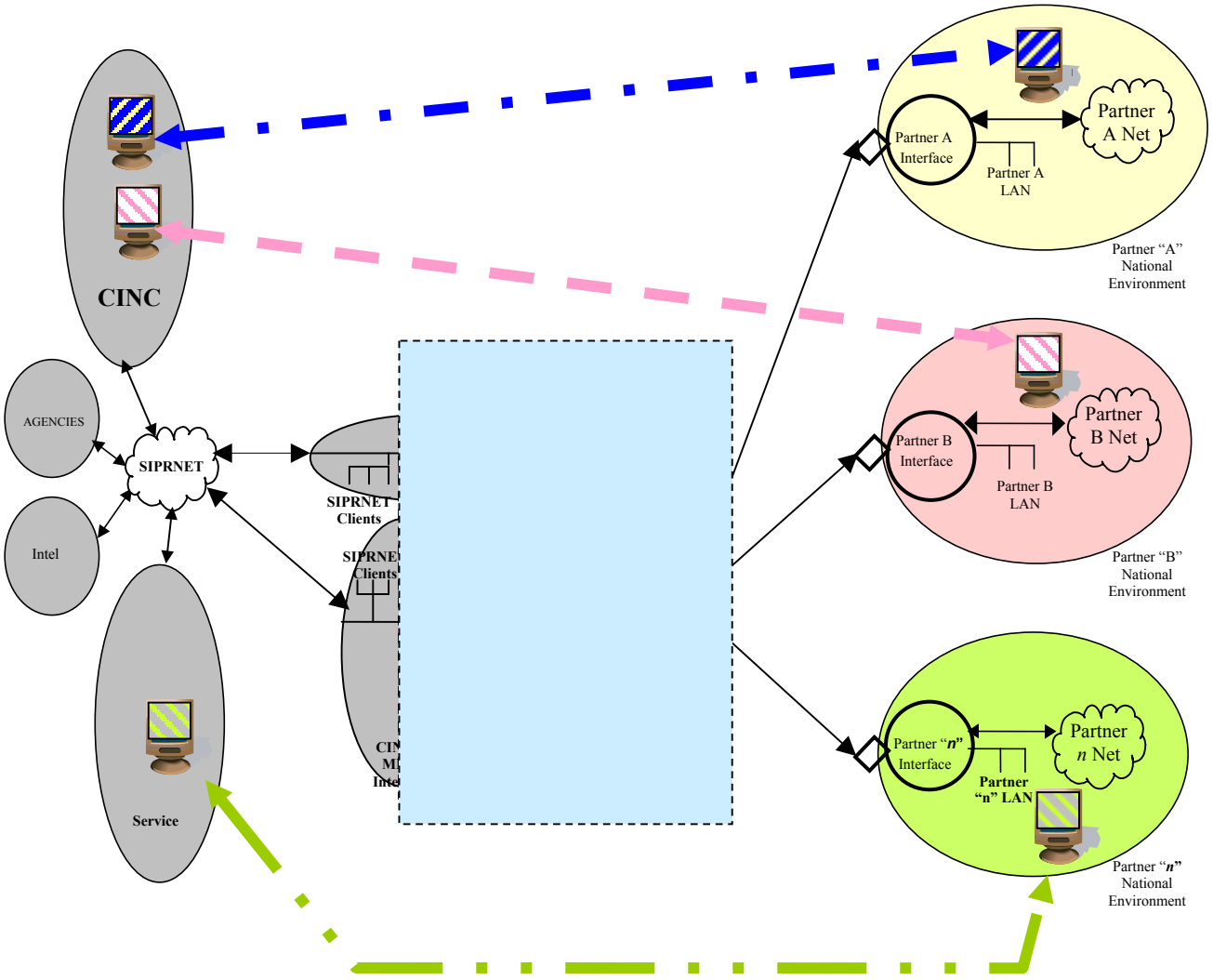


Figure 6 - Support for Bilateral Communication Paths

Even though the MNIS model and TOE specified by this PP aren't intended to support high assurance separation of bilateral communications, authorized MNIS users and partners can use the COI access control tools included in the TOE to keep their less sensitive (limited distribution

based on need-to-know) bilateral communications separate within the MNIS Information Domain.

Historically, bilateral communication occurs via links that are separate from multinational infrastructures connecting specified partners. In the case of the MNIS environment, these existing bilateral connections might coexist in parallel to the proposed MNIS TOE as shown in Figure 6 above. When bilateral connections are incorporated in Combatant Command environments, which also include MNIS connectivity, appropriate data separation and transmission security mechanisms must be selected in accordance with applicable security policy and procedures as negotiated with the specific partner. Specification and selection of appropriate mechanisms for bilateral connectivity are not included in this PP.

2.3 MNIS TOE Functional Security Architecture

This section describes the MNIS TOE functional security architecture. In keeping with the goals of a protection profile, specific implementation details are not included. In an actual implementation, various combinations of components may be integrated to provide the entire TOE functionality.

The TOE functional security architecture is complex and includes elements that are physically located in multiple environments. The TOE provides protection, detection, and reaction mechanisms to address the threats and vulnerabilities associated with each physical environment, which contains TOE elements. In addition, TOE security elements include functionality to protect both the processing of information contained within the MNIS Information Domain, and also to provide for a controlled interface and interconnection of the MNIS Information Domain to dissimilar information domains. The controlled interface between information domains consists of more than just a security guard system. The security features associated with the interconnection between information domains are distributed across the TOE functional architecture. Thus, this protection profile is based on a system perspective where security features in the clients, servers, applications, and guard systems are combined to mitigate the risks of interconnecting information domains.

This PP does not specify security functionality for the partner environments. Each partner is responsible for protecting its own information systems. However, to connect to the MNIS Information Domain protected by the TOE, each partner agrees to comply with specified security requirements that are discussed in this PP. See also Section 6.5.3.

Security functionality within the security architecture can be grouped into four broad categories as shown in Figure 7. They are Access Control, Transmission Security, Cross-Domain Filtering, and Security Administration. Some of the security functionality will be supported by the TSE (TOE Security Environment) and will be discussed in the next chapter.

2.3.1 Access Control

Access control security functions enforce rules that specify who or what can access and use systems, hardware, information, or resources. Also, access to all access control security functions, rule sets, and components must be controlled. Access control functionality enforces individual and group access to systems, hardware, information, or resources by doing the following:

- Access controls separate COIs (information subdomains) within an information domain. Security functionality authenticates each user prior to granting the user access to an authorized information domain or subdomain.
- Access control functions maintain the confidentiality and integrity of information during storage and processing within the MNIS information domain. These functions help ensure that information is not disclosed or changed without authorization.
- Each person or process that is authorized access to the MNIS Information Domain, including those authorized to send or receive information across the MNIS domain boundary, must be uniquely identified.

Access controls may include electronic, cryptographic, physical, and procedural elements. The choice of element to provide a given access control function is based on the sensitivity of the controlled system, information, or resource, the duration of protection required, and an analysis of the threats against the system, information, or resource. Within the MNIS Information Domain, medium robustness access controls are sufficient to separate COI information subdomains.

2.3.2 Transmission Security

One role of transmission security is to maintain the confidentiality and integrity of information during transfer across the physical environments of the TOE and between information domains. Transmission security may also be used to implement COI separation within the MNIS Information Domain.

2.3.3 Cross-Domain Filtering

Cross-domain filtering includes all security functions necessary to transition/regrade information from one domain to another in accordance with applicable security policies. While the majority of the cross-domain filtering elements are contained within a boundary protection device, this functionality will require support from procedural controls, elements and applications interfacing to the boundary protection device.

Cross-domain filtering support functions (such as document generation, review, and release activities) prepare information for transmission across a domain boundary. Although they may operate outside of the TOE, the TOE must validate the filtering support functions that were

performed by these applications. Similarly, some of the applications that receive information that has crossed a domain boundary are not within the TOE. Regardless of whether these applications are in the TOE or in the TSE, they are responsible for accepting valid information.

Security boundary components provide validation, filtering, and transfer mechanisms that comply with current DoD domain transfer policies. These mechanisms ensure that the information is in an authorized format, carries a proper sensitivity label, has been released by an authorized user or process, contains a valid integrity seal, and is addressed to an authorized recipient user or process. The filter mechanisms must be able to scan the content of the information for unauthorized content, including malicious code. If possible, the filter mechanisms reformat or sanitize the information in accordance with applicable security policies or will alternatively reject the transmission and make appropriate notification. The security boundary component must regrade the information authorized for transfer to another information domain. The filter mechanisms must block the transfer of all information that is not authorized and generate appropriate audit records of these actions.

Information systems and applications must interpret information that indicates sensitivity and releasability decisions, to include labels created by one or more of the partners. All information systems and applications within the MNIS information domain will have the capability to preserve or suppress the identity of the partner that transferred the information into the MNIS information domain in accordance with negotiated security policy.

2.3.4 Security Administration

In general, the U.S. will administer the security policy in the U.S.-only environment and the MNIS environment. However, the U.S. may authorize an agent to administer the MNIS environment. The following security administration functions shall be implemented in the MNIS TOE.

Within the TOE, auditing functions provide TOE Security Administrators the ability to record selected system events and generate appropriate audit records. At a minimum, the following events will be audited: events related to the cross-domain transfer of information, events related to security administration, user authentication, denial of access events, and installation or removal of software or hardware. The auditing function identifies all unauthorized use of the system, whether by authorized or unauthorized personnel and all security-relevant events. Audit records generated by the TOE support forensic investigation and analysis after a perceived intrusion.

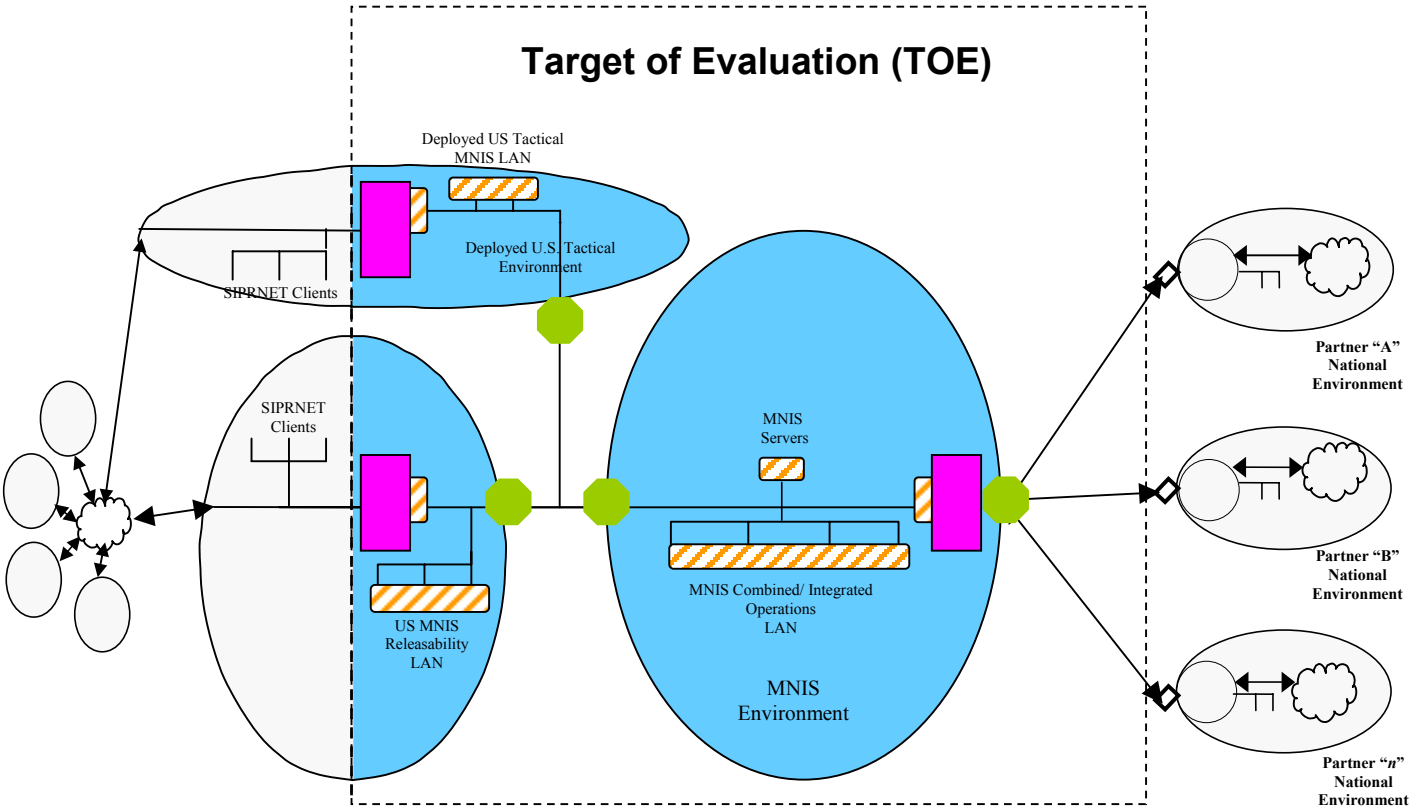
The Security Administrator for the TOE shall evaluate the security of the TOE at least annually. This evaluation shall include system penetration testing, security exercises, formal accounting of software and hardware components, and an independent review of security procedures. Based on the results of the evaluation, the security manager shall improve the TOE security policy, security functions, and user training.

All hardware and software shall be accounted for automatically and security managers shall track the configuration of all hardware, software, and databases. Automated component scanning and tracking tools may be used.

Comprehensive and current intrusion detection, malicious code detection, and anomaly event detection shall be used. Detection systems must alert appropriate officials via real time and other means as appropriate. The detection of unauthorized activity associated with circumventing security settings shall immediately alert security officials. Systems shall be able to detect when any of the partners attempts to exceed its authorized access.

Incident reaction functions may include the ability to segregate suspicious activity, restrict access to a predetermined list of users, terminate applications, protocols, or services, or disconnect capabilities, or notify partners as determined by security officials. Contingency and incident recovery systems must restore operations as quickly as possible after operational degradation. Principal systems must operate during power outages. Backups of operational data and software shall be available to allow for the rapid restoration of data and systems.

Security updates and maintenance must occur in accordance with policy. Users, maintainers, and administrators are trained on current security policies and procedures. TOE Security Administrators review and update security policies and procedures as necessary.



	Cross-Domain Filtering Functions
	Transmission Security Functions
	Access Control Functions
	Security Administration Functions
	TOE Boundary

Figure 7 - MNIS TOE Functional Security Architecture

3 - TOE Security Environment (TSE)

As previously explained for the purpose of this PP, the TOE will focus on the security functionality allocated to components contained within the MNIS Information Domain. Supporting the TOE however there is additional security functionality that is required which is considered included within the TOE Security Environment (TSE).

External to the TOE, but within the TSE, supporting security functionality might include (but is not limited to) key and privilege management support infrastructures, additional audit detection/analysis/reaction capabilities, information pre-processing/filtering/labeling infrastructures, etc.

This PP will not analyze or specify the security functional requirements that must be provided within the TSE in support of the TOE but will attempt to codify security objectives applicable to the TSE which might be considered by SSEs while crafting a specific security implementation for unique customer requirements.

The following naming conventions are used for TOE Security Environment threats, policies, and assumptions:

- Threats are given names beginning with "T." and are presented in alphabetical order, e.g., T.ALARM_FAIL, T.IMPORT.
- Policies are given names beginning with "P." and are presented in alphabetical order, e.g., P.NEED_TO_KNOW, P.TRAINING.
- Assumptions are given names beginning with "A." and are presented in alphabetical order, e.g., A.ENCRYPT, A.NOPUBLIC.

3.1 Threats to the TOE

The following list of threats result from a security analysis relevant to the information contained within the MNIS Information Domain and the resources included in the physical environments which contain the TOE.

Subsequent sections of the PP will describe both relevant assumptions which may contribute to the mitigation of these threats, and security objectives for the TOE that are intended to address the residual risk resulting from these threats. The determination of adequate threat mitigation is addressed in Chapter 6, Rationale.

The possible damage associated with the following threats may be motivated by deliberate malice or could be the result of unintentional mistakes.

The threats listed below are those that are addressed by a TOE that is compliant with this Protection Profile. The term "compromise" (when unqualified) refers to a degradation of the confidentiality, availability, and/or integrity of an asset.

T.ACCESS_ELECTRONIC - An unauthorized agent may gain network access to the TOE and thereby compromise its secure operation.

T.ACCESS_PHYSICAL[19] - An unauthorized agent may gain physical access to the TOE and thereby compromise its secure operation.

T.ALARM_FAIL Failure of intrusion detection systems, alerting systems, or alarms may allow unauthorized activity to occur without detection or security response.

T.AUDIT_FAIL System modification, compromise, or audit file "full" may result in an audit failure.

T.AUTHORIZATION_EXCEED - Authorized users may access data or resources for which they are not authorized.

T.COMPROMISE_CRYPTO - Unauthorized agents may attack TOE cryptographic components using cryptanalysis or social engineering and compromise the secure operation of the TOE.

T.DENIAL_OF_SERVICE - An unauthorized agent may intentionally compromise the availability of the TOE with a denial of service attack.

T.DISASTER_ENVIRO - Environmental disasters may compromise the secure operation of the TOE.

T.ERROR_ADMIN TOE administrator error may violate security policy, compromise information, or degrade secure TOE operation.

T.ERROR_USER An authorized user may perform erroneous actions that will violate security policy, compromise information, or corrupt information integrity.

T.IMPERSONATE An unauthorized agent may attempt to gain network access to the TOE or the information it protects by pretending to be an authorized user or administrator.

T.IMPORT_BAD Unauthorized code, to include malicious code, may be introduced into the TOE, resulting in a compromise to its secure operation.

T.MALICIOUS_ADMIN - Occasionally an administrator maliciously attempts to compromise information or undermine the function of the TOE.

[19] This threat includes the situation where personnel may be authorized access to the room in which the TOE is located but not be authorized to have physical access to the actual TOE components (e.g., custodial personnel).

T.MALICIOUS_USER - Occasionally an authorized user maliciously attempts to compromise information or undermine the function of the TOE.

T.POOR_ADMIN Poor systems and security administration may compromise the secure operation of the TOE. For example, administrators may fail to review configuration settings periodically, install system and security patches, or take appropriate actions in response to audit analysis alerts.

T.POOR_BACKUP Failure to adequately perform system backup may result in compromise of TOE operation or loss of user data.

T.POOR_IMPLEMENTATION - Due to poor design or improper implementation of the TOE it may not operate in a secure manner.

T.POOR_TRAIN Insufficient training may result in insecure operation of the TOE.

T.REPUDIATE Authorized users or administrators may deny performing actions that they did perform.

T.TOE_FAIL TOE component or software failure may cause the TOE to operate in an insecure manner.

3.2 Organizational Security Policies

The following statements identify and explain organizational policies/rules that are relevant to the TOE. These policies define the operation, management, personnel responsibilities, and guidelines that the sponsoring U.S. Command, Service, or Agency must enforce to provide security for the TOE.

Subsequent sections of the PP will describe relevant assumptions, which may contribute to satisfying portions of the identified policies and will modify the impact of these policies on identified security objectives for the TOE.

P.ACCOUNTABILITY - Authorized administrators and users are held accountable for security relevant actions they perform.

P.ADMIN_SECURITY - A Security Administrator interprets, maintains, and oversees site security policy and develops and implements procedures assuring secure operation of the TOE.

P.ADMIN_SPLIT Administrative responsibilities are split between System Administrator and Security Administrator roles that together competently administer the TOE. The assignment of split administrative authorization is established in order to prevent unrestricted system control and to provide for “checks and balances.”

P.ADMIN_SYSTEM - A System Administrator is responsible for installing, configuring, managing, and monitoring the performance of the TOE in accordance with

its evaluated configuration and ensuring its conformance to applicable security policies.

P.AUDIT_REVIEW Administrators and users will review audit reports and take appropriate action.

P.CROSS_DOMAIN_FILTERING - Information domains will not be directly connected without application of appropriate cross-domain filtering techniques.

P.DISTRIBUTION A Security Administrator will issue security relevant TOE hardware and software, and will maintain all records regarding distribution of these items.

P.DUE_CARE The level of security afforded the IT system must be in accordance with what is considered prudent by the organization's accrediting authority. This authority will assure that the organization's IT systems are implemented, maintained, and operated in a manner that represents due care and diligence with respect to usage issues and risks to the organization.

P.MNIS_ENVIRON_EXTERNAL_DISTRO - Confidentiality and integrity protection must be applied to information transferred into and out of the MNIS environment.

P.MNIS_ENVIRON_INTERNAL_DISTRO - The MNIS environment is a physically protected system high environment for Secret MNIS information. Transmission security is not required within the protected environment, but access controls are necessary.

P.MNIS_INFO_PROTECT - All information processed or stored internal to the MNIS Information Domain will be protected as Secret with appropriate releasability caveats.

P.MNIS_INFO_RECIPIENTS - U.S. and partner personnel and processes that are recipients of information transferred out of the MNIS Information Domain must be explicitly authorized to receive it.

P.MNIS_INFO_SENDERS - TOE users and processes must be explicitly authorized to transfer information outside the MNIS Information Domain.

P.MNIS_INFO_SOURCES - U.S. and partner personnel and processes that transfer information into the MNIS Information Domain must be explicitly authorized to do so.

P.REJECT_PARTNER_INFO - The TOE will check all information it receives from partner sources. It will return and not allow information into the MNIS Information Domain that it determines to be outside the bounds of negotiated partnership information agreements.

P.REJECT_U.S._INFO - The TOE will check all information it receives from U.S. sources. It will return and not allow information that it determines to be higher than

Secret or not releasable, to be processed or stored within the MNIS Information Domain.

P.SECURITY_ADMIN_RESTRICTED - Only authorized System Administrators, Security Administrators, and their representatives may administer or repair security mechanisms (e.g., the cross-domain filtering function) in the TOE.

P.USERS Only personnel authorized by the sponsoring U.S. Command, Service, or Agency may have access to or utilize TOE resources.

3.3 TOE Assumptions

The following assumptions result from an analysis of assumptions relevant to mitigation of identified threats to the TOE and policies that the TOE must support. These assumptions are relevant to protection of the information contained within the MNIS Information Domain and the resources included in all of the physical environments in which the TOE is contained.

A.ADMIN_AVAILABLE - At least one Security Administrator authorized by the U.S. is available at all times to respond to TOE security incidents, alerts, and alarms.

A.AUDIT_ANALYSIS - Mechanisms exist outside the TOE but within the TSE to perform sophisticated audit analysis (e.g., audit reduction and trend analysis) to augment TOE capability.

A.BACK_UP Back ups of TOE files and configuration parameters are performed as required in accordance with site security policy. They are sufficient to restore TOE operation in the event of a failure or security compromise. Back ups are transparent to the user and performed automatically on a timely basis as determined by site policy.

A.CLEARANCE All authorized users and administrators with access to the TOE will be authorized by their government to have access to, and the need-to-know, Secret classified information.[20]

A.COI Community of Interest (COI) information sub-domains shall be supported by protection mechanisms adequate to provide data separation and segregation based on need-to-know and will be implemented with medium robustness security.

A.COMMS_AVAILABLE - Adequate communication capability exists between TOE physical environments.

[20] For U.S. users this is defined by DoD Directive 5200.2, *DoD Personnel Security Program*. For foreign partners this is defined by DoD Directive 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*.

A.COMPLY The implementation and use of the organization's IT systems complies with all applicable laws, regulations, licensing agreements and negotiated multinational security policy.

A.CONFIGURATION - The U.S. proposes products and standards and negotiates their selection with partner nations. The U.S. or its designee enforces the configuration control of these items.

A.CONNECTIONS The U.S. will install and manage all connections between U.S.-only environments and the MNIS environment. In accordance with the negotiated agreements, the U.S. or its authorized agent will install and manage connections between the MNIS environment and each partner.

A.CRYPTO_SUPPORT - Cryptographic support infrastructure will be provided by procedures and mechanisms external to the TOE, within the TSE (e.g., user registration, key issuance, directory services, and assignment of privileges).

A.DYNAMIC_PARTNERSHIP - The membership of the multinational partnership is dynamic.

A.INFORMATION_VALUE - The value of information is equivalent to V4[21] where the violation of the information protection policy would cause serious damage to the security, safety, financial posture, or infrastructure of the U.S., its multinational partners, or operations.

A.LOGISTICS_SUPPORT - Logistics support will be planned and implemented to ensure that sufficient spare parts are available to quickly restore service to the TOE when failures occur.

A.MISSION TOE users will co-operate to achieve a common multinational mission.

A.MNIS_INFO_ACCESSIBLE - All internal MNIS environment communication connections have adequate physical protection commensurate with the need to protect Secret MNIS information. Therefore, transmission security protection is not required but access controls are.

A.MNIS_INFO_CLASSIFICATION - All information processed or stored internal to the MNIS Information Domain is assumed to be classified no higher than Secret with appropriate releasability caveats.

A.MNIS_INFO_INTERNAL - All TOE users and processes located within the MNIS Information Domain may freely exchange information within the same domain and/or COI.

A.PERSONNEL_TRUST - Users and administrators are typically trusted to perform their duties competently and in accordance with established policy, however occasionally prove to be untrustworthy.

[21] Value of information V4 is defined in the "*Information Assurance Technical Framework*", Release 3, Section 4.5 "Robustness Strategy", National Security Agency, September 2000. See also http://www.iatf.net/.

A.PHYSICAL_SECURITY - The TOE components are located within controlled access areas that provide protection against unauthorized physical access and tampering by unauthorized agents.

A.POLICY_MNIS The U.S. negotiates MNIS information domain policy with the partner nations and enforces, or delegates enforcement of, it.

A.POLICY_US_REL-LAN - U.S. personnel establish and enforce policy within the U.S.-ONLY Releasability LAN. This policy incorporates negotiated MNIS Information Domain policy.

A.SPONSOR A U.S. military Command, Service, or Agency sponsors the MNIS environment and the interconnections between it and the U.S. and partner environments and provides the personnel and resources necessary to securely interconnect and operate the MNIS environment.

A.SYSTEM_HIGH The TOE operates in the system-high mode. TOE users have valid security clearance for all of the multinational information but do not have need-to-know for all of the information contained within the MNIS Information Domain.

A.TEMPEST The TOE will be installed in a protected environment and will not require any additional TEMPEST protection

A.THREAT_LEVEL Within the MNIS environment the threat agent is a passive adversary with minimal resources who is willing to take little risk (T2[22]). Between sub-environments of the MNIS Information Domain, the threat agent is a sophisticated adversary with at least moderate resources who is willing to take significant risk (T5[23]).

A.TOE_DESIGN The TOE is designed, manufactured, installed, and configured in accordance with its evaluated configuration and conforms to applicable security policies.

A.TOE_MAINTENANCE - The TOE will be maintained by the System Administrator or by designated maintenance personnel who have been properly cleared and trained, and who perform under the supervision of the System Administrator.

A.TOE_OPERATION - The TOE is operated, maintained, and managed in accordance with its accredited configuration and conforms to applicable security policies.

A.TOE_USER TOE users will be either U.S. or partner nation personnel who have been specifically authorized to participate in the multinational operation or mission.

---

[22] Threat T2 is defined in the "*Information Assurance Technical Framework*", Release 3, Section 4.5 "Robustness Strategy", National Security Agency, September 2000. See also http://www.iatf.net/.

[23] Threat T5 is defined in the "*Information Assurance Technical Framework*", Section 4.5.

A.TOE_USER_AUTHENTICATION - The TOE will authenticate the identity of each authorized TOE user prior to granting access privileges to TOE assets and information contained within the MNIS Information Domain.

A.TRAINED All users, administrators, and maintainers are appropriately trained.

A.TRANSEC_CRYPTO - Cryptographic methods used in the TOE between environments will be resistant to attacks and be of adequate strength and robustness to protect Secret classified data.

A.UNMARKED_INFORMATION - Unmarked information transferred into the MNIS Information Domain is assumed to be classified by the country of origin as Secret releasable to all partners.

4 - Security Objectives

Section 4.1 lists the security objectives for the TOE. Each objective reflects the stated intent of the TOE to either counter the threats identified or adhere to applicable policies while taking into consideration the relevant defined assumptions. The rationale for each objective is presented in Section 6.2.

Likewise, Section 4.2 lists the security objectives for the TOE security environment (TSE) that may be traced to identified threats that elements of the TSE will counter and/or policies the TSE elements will support.

Naming convention for objectives: security objectives for the TOE and the TSE are given names beginning with "O." and "OE." respectively, and are presented in alphabetical order, e.g., O.AUDIT, O.RESIDUAL_INFORMATION, OE.BACKUP, OE.SPLIT_ADMIN.

4.1 Security Objectives for the TOE

O.AUDIT The TOE will monitor and generate accurate audit records of security relevant events.

O.AUTHENTICATION - The TOE must authenticate the identity of each user and administrator prior to granting access to, or use of, the TOE and its resources in accordance with their authorizations.

O.AUTHORIZED_USE - The TOE must ensure that only uniquely identified users and administrators authorized by the sponsoring U.S. Command, Service, or Agency may utilize, administer or repair the TOE and its resources within the limits of their authorization.

O.CROSS_DOMAIN_FILTERING - The TOE will include appropriate cross-domain filtering and authentication techniques between the MNIS Information Domain and external information domains, users, and processes. The TOE Cross-Domain Filtering function will allow only releasable information classified no higher than U.S.-Secret into the MNIS Information Domain.

O.ERROR_REJECT The TOE must ensure that administrator or user error will not result in a violation of security policy, information compromise, a corruption of information integrity, or a degradation of secure TOE operation.

O.MANAGE The TOE must incorporate user friendly mechanisms to ensure secure administration of its operation.

O.NON-REPUDIATION - The TOE must accurately and dependably attribute actions performed by authorized users or administrators.

O.PROHIBIT_MALICIOUS_CODE - The TOE must detect and prohibit attempts to introduce unauthorized or malicious code or applications into the TOE.

O.PROTECT The TOE must protect against authorized users and administrators compromising information or degrading the secure operation of the TOE.

O.PROTECT_EXT_COMMS - The TOE must include confidentiality and integrity protection between physically distributed environments of the TOE and between the TOE and partner environments.

O.REACT The TOE will react to misuse detection analysis that is performed within the TSE and alert TOE administrators (e.g., detected viruses, unauthorized use, or audit file "full" conditions).

O.RECOVERY The TOE must include mechanisms and implement predefined procedures to ensure that it is restored to a secure operational state following recovery from system failure.

O.TOE_FAILSAFE The TOE must immediately react to specified security critical events and enter a secure state.

4.2 Security Objectives for the TSE

OE.ACCESS_PHYSICAL - The TSE must include mechanisms and procedures that ensure the physical protection of the TOE from unauthorized agents.

OE.AVAILABILITY_OF_SERVICE - The TSE will detect attempts to deny TOE information and services to authorized users and administrators and will respond appropriately.

OE.BACKUP The TSE must ensure that adequate system backups are regularly performed in accordance with TOE policy and procedures.

OE.DISTRIBUTION TSE procedures must ensure that TOE administrators issue security relevant TOE hardware and software to appropriate personnel, maintain inventory records of these items, and track the return or disposal of these items.

OE.DUE_CARE Administrators will periodically ensure that the implementation, maintenance, and approved operating procedures for the TOE represent due care and diligence with respect to risks and threats, and that they comply with the organization's accrediting authority.

OE.GOOD_ADMIN Administrators of the TOE will periodically review configuration settings, ensure all current software patches are installed, and appropriately respond to alarms and audit analysis results.

OE.MISUSE_DETECTION - The TSE must include the capability to interpret audit records, perform audit analysis, and generate audit alert for subsequent action.

OE.PROTECT_SECRETS - Procedures must be established that will inhibit unauthorized agents from using social engineering techniques to gain security relevant information (e.g., passwords) about the TOE and the information it protects.

OE.SPLIT_ADMIN The TSE must include mechanisms to ensure that the administration of the TOE is appropriately split between the defined roles of TOE System and Security Administrators.

OE.SPLIT_ADMIN_SECURITY - A Security Administrator interprets, maintains, and oversees site security policy and develops and implements procedures assuring secure operation of the TOE.

OE.SPLIT_ADMIN_SYSTEM - A System Administrator installs, configures, manages, and monitors the performance of the TOE, ensuring that the TOE complies with its evaluated configuration and conforms to applicable security policies.

5 - TOE Security Requirements

This chapter provides the TOE security functional requirements and security assurance requirements. The security functional requirements for TOE information technology (IT) systems are grouped into the four categories that were discussed in Section 2.3: access control, cross-domain filtering, security administration, and transmission security. Next, some non-IT security requirements are also presented, followed by the TOE security assurance requirements. But first, Section 5.1 explains the conventions used in this chapter.

5.1 Conventions

The notation, formatting, and conventions used in this protection profile (PP) are based on or consistent with version 2.1 of the *Common Criteria* (CC). Font style and clarifying information vehicle conventions were developed to aid the reader.

A font style convention was developed so that protection profiles will be consistent in the presentation of functional component operations. The family behavior name is followed by the family short name in parentheses, and the short family name is superscripted following the requirement statement. Example:

Audit Review (FAU_SAR.1)
The TSF shall provide [an authorized administrator] with the capability to read [all trail data] from the audit records. FAU_SAR.1.1

The CC permits four functional component operations—assignment, iteration, refinement, and selection—to be performed on functional requirements. These operations are defined in Part 2 of the Common Criteria, paragraph 2.1.4 as:

- assignment: allows the specification of an identified parameter;
- iteration: allows a component to be used more than once with varying operations;
- refinement: allows the addition of details; and
- selection: allows the specification of one or more elements from a list.

With the exception of iteration, these operations are expressed by using bolded, italicized, and underlined text. The author used brackets ("[]") to set off all assignments or selections that require future action by the developer. The text "assignment:" or "selection:" is indicated within the brackets. Iterations are set off with parentheses. The iteration "(#)" follows the short family name and "(iteration #)" follows the family behavior.

Table 1 - Functional Requirements Operation Conventions

Convention	Purpose	Operation
Bold	The purpose of bolded text is used to alert the reader that additional text (a "Refinement") has been added to the standard CC language. This could represent either additional explanatory information or completion of an "Assignment" from the CC. Example: The TSF shall export **(in ASCII format)** the **labeled** user data with the user data's associated security attributes.	Assignment Refinement
Italics	The purpose of italicized text is to inform the reader of an appended assignment or selection operation to be completed by the developer. Example: The TSF shall provide the following [assignment: *list of additional SFP capabilities*].	Assignment Selection
Underline	The purpose of underlined text is to inform the reader that a choice was made from a list provided by the CC selection operation statement. Example: The TSF shall be able to prevent modifications to the audit records.	Selection
Bold & Italics	The purpose of bolded and italicized text is to inform the reader that the author has added new text to the requirement and that an additional vendor action needs to be taken. Example: **Subject sensitivity label; Object sensitivity label; [assignment: *list of additional attributes that audit selectivity is based upon*].**	Assignment Refinement

Convention	Purpose	Operation
Parentheses	The purpose of using parentheses and an iteration number is to inform the reader that the author has selected a new field of assignments or selections with the same requirement and that the requirement will be used multiple times. Example: Basic data exchange confidentially (Iteration 1) FDP_UCT.1(1) The TSF shall enforce the **[policies P.ADMIN ACCESS and P.USER ACCESS]** to be able to transmit objects in a manner protected from unauthorized disclosure.[FDP_UCT.1.1] Basic data exchange confidentially (Iteration 2) FDP_UCT.1(2) The TSF shall enforce the **[policies P.ADMIN ACCESS and P.USER ACCESS]** to be able to receive objects in a manner protected from unauthorized disclosure.[FDP_UCT.1.1]	Iteration

Convention	Purpose	Operation
Endnotes	The purpose of endnotes is to alert the reader that the author has deleted CC text. An endnote number is inserted at the end of the requirement, and the endnote is recorded in the last annex to the document. The endnote statement first states that a deletion was performed, and then provides the rationale. Following is the family behavior or requirement in its original and modified form. A strikethrough is used to identify deleted text and bold for added text. A text deletion rationale is provided. Examples: Text as shown: **Guarantees of audit data availability** (FAU_SGT.1) **1** Endnote statement: A deletion of CC text was performed. Rationale: The component name was changed to… ~~Protected audit trail storage~~ **Guarantees of audit data availability** (FAU_SGT.1) Text as shown: The TSF shall **be able to** prevent auditable events, except those taken by the authorized administrator, and **[assignment: *other actions to be taken in case of audit storage*]** if the audit trail is full. (FAU_STG.4.1) **2** Endnote statement: A deletion of CC text was performed. Rationale: The words "with special rights" were deleted because… The TSF shall **be able to** prevent auditable events, except those taken by the authorized administrator ~~with special rights~~, and **[assignment: *other actions to be taken in case of audit storage*]** if the audit trail is full. (FAU_STG.4.1)	Refinement

Convention	Purpose	Operation
(EXP)	The purpose of using (EXP) after the family behavior name is to alert the reader to and explicitly identify a newly created requirement. Example: Object security attributes (EXP) (FDP_OSA.1) The TSF shall associate the following security attributes with named objects: a) Access control attributes, consisting of the following [assignment: *list of object attributes used to enforce the Discretionary Access Control Policy*.] b) Sensitivity label consisting of a hierarchical level and a set of non-hierarchical categories c) [assignment: *other object security attributes*]. (EXP) (FDP_OSA.1.1)	Refinement

As a means to provide the reader with additional requirement understanding or to clarify the author's intent, requirements overview and application notes are used.

The requirements overview are used to provide a discussion of the relationship between functional requirements so that the protection profile reader can understand why a component or group of components were chosen and what effect they are expected to have as a group of related functions. The requirements overview precedes either a component or a set of components.

To provide support information that is considered relevant or useful for the construction, evaluation, or use of the TOE, (e.g., to clarify the intent of a requirement, to identify implementation choices, or to define "pass-fail" criteria for a requirement) application notes are used. Application notes follow the relevant requirement component.

5.2 TOE Security Functional Requirements

The unique nature of the TOE creates interpretation problems for traditional information technology and information security terminology. The CC defines security requirements for information technology and security without regards to unusual IT environments. The nature of this document is to define an "implementation independent" set of requirements to address information security features and controls.

Terminology such as "session", "login", or "user accounts" is intended to convey traditional methods of discrete computer processing sessions, individual identification and authentication and access control features. The Security Target (ST) writer may choose to implement or recommend different terminology to describe equivalent concepts. This is permissible provided

the ST writer describes the intent of each term and the corresponding impact on information security.

Terminology such as “user data” is intended to identify any data or information that is transmitted, processed, or stored by the TOE that is not specifically TSF (TOE Security Function) related.

The contractor shall follow DIA, DoD, and Service policies, guidance, and directives when providing specifications for any of the requirements within this Protection Profile.

The contractor software development practices shall meet the intent of DoD 5220.28-M, NISPOM, *National industrial Security Program Operating Manual* and DoD 5220.28-M Sup 1, NISPOMSUP, *National Industrial Security Program Operating Manual Supplement*, February 1995.

The contractor software development practices shall meet the intent of National Security Telecommunications and information Systems Security Policy (NSTISSP) No.11, National Information Assurance Acquisition Policy, January 2000.

The contractor software development practices shall meet the intent of DoD information and Assurance Guidance and Policy Memorandum.

5.2.1 Access Control

5.2.1.1 Security Audit (FAU)

5.2.1.1.1 Audit Data Generation (FAU_GEN.1)

5.2.1.1.1.1 The TSF shall be able to generate an audit record of the following auditable events: FAU_GEN.1.1

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [basic] level of audit;
c) The events in the table (below):

Table 2 - Audit Events for Access Control

Functional Component	Auditable Event	Additional Audit Record Contents (beyond those in FAU_GEN.1.2)
FDP_ACC.2	All requests to perform an operation by a subject or on an object covered by the policy.	If access was denied, the reason the TSF blocked the operation.
FDP_ACF.1	All requests to perform an operation on an object covered by the policy.	If access was denied, the reason the TSF blocked the operation.
FDP_IFC.2	(None)	(None)
FDP_IFF.2	All decisions on requests for information flow.	The address of the presumed sender and recipient(s), and, if the information flow was denied, the reason the TSF denied it.
FDP_ITT.2	All attempts to transfer user data, including the protection method used and any errors that occurred.	(None)
FDP_RIP.1	(None)	(None)
FDP_UCT.1	All attempts to use the data exchange mechanism.	The names or other indexing information useful in identifying the user data that was transmitted or received.
FDP_UIT.1	All attempts to use the data exchange mechanism. Any attempt to block transmission of user data.	The names or other indexing information useful in identifying the user data that was transmitted or received.
FIA_AFL.1	Reaching the threshold for unsuccessful authentication attempts and the actions taken, and the subsequent restoration to normal operational state.	The identity being presented, the identity of the terminal or communication channel, and the identity of the administrator that restored the system to normal operation.
FIA_ATD.1	(None)	(None)
FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret.	(None)

Functional Component	Auditable Event	Additional Audit Record Contents (beyond those in FAU_GEN.1.2)
FIA_UAU.2	All use of the authentication mechanism.	The user identity being presented.
FIA_UAU.6	All reauthentication attempts.	(None)
FIA_UAU.7	(None)	(None)
FIA_UID.2	All use of the user identification mechanism, including the user identity provided.	The user identity being presented.
FIA_USB.1	Success or failure of binding of user security attributes to a subject (such as success or failure to create a subject).	The subject identity, the security attribute(s), and the binding result.
FMT_MOF.1	All modifications in the behavior of the functions in the TSF.	(None)
FMT_MSA.1 (Iteration 1)	All modifications of the values of security attributes.	(None)
FMT_MSA.1 (Iteration 2)	All modifications of the values of security attributes.	The names or other indexing information useful in identifying the object whose security attributes were modified.
FMT_MSA.2	All offered and rejected values for a security attribute.	The value being offered and reason for rejection.
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules and all modifications of the initial values of security attributes.	(None)
FMT_MTD.1	All modifications to the values of TSF data.	(None)
FMT_REV.1	All attempts to revoke security attributes.	(None)
FMT_SMR.2	Modifications to the group of users that are part of a role. Unsuccessful attempts to use a role due to the given conditions on the roles.	Reason for failure to use the role.
FMT_SMR.3	Explicit request to assume a role.	(None)
FPT_AMT.1	Execution of the tests of the underlying machine and the results of the tests.	Reason the test execution cannot be completed.
FPT_FLS.1	Failure of the TSF.	The identity of the failed mechanism(s) and the reason for failure, if discernable.
FPT_PHP.2	Detection of tampering.	Reason for detection and action taken in response.
FPT_RCV.2	Type of failure or service	Whether automatic recovery was

Functional Component	Auditable Event	Additional Audit Record Contents (beyond those in FAU_GEN.1.2)
	discontinuity.	successful or not and reason for inability to automatically recover, if discernable.
FPT_RPL.1	Detected replay attack.	The identity being presented, the identity of the terminal or communication channel, and the signature of the attack.
FPT_RVM.1	(None)	(None)
FPT_STM.1	Changes to the time.	(None)
FPT_TDC.1	Use of the TSF data consistency mechanism and detection of modified TSF data.	Modified TSF data content and reason for detection.
FPT_TST.1	Execution of the TSF self tests and the results of the test.	The reason for execution of the test(s) and the test results.
FTA_MCS.1	Rejection of a new session based on the limitation of multiple concurrent sessions.	(None)
FTA_SSL.1	Any attempts at unlocking an interactive session.	The approach taken to unlock the session if the user was unsuccessful in unlocking the session normally.
FTA_SSL.2	Any attempts at unlocking an interactive session.	The approach taken to unlock the session if the user was unsuccessful in unlocking the session normally.
FTA_SSL.3	Termination of an interactive session by the session locking mechanism.	Account identifier and reason for session termination.
FTA_TAH.1	(None)	(None)
FTA_TSE.1	All attempts at establishment of a user session.	Reason session establishment was denied.

5.2.1.1.1.2 The TSF shall record within each audit record at least the following information:
FAU_GEN.1.2

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST:
   - [The sensitivity label attached to applicable objects,
   - The before and after value(s) of changed configuration settings, lists, or tables,
   - The identity of the user or administrator who made the change,
   - {*And other user attributes and data chosen by the Security Target author*}].

5.2.1.1.2 User Identity Association (FAU_GEN.2)

5.2.1.1.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event. FAU_GEN.2.1

5.2.1.2 User Data Protection (FDP)

5.2.1.2.1 Complete Access Control (FDP_ACC.2)

5.2.1.2.1.1 The TSF shall enforce the [mandatory access control policy] on [subjects and objects] and all operations among subjects and objects covered by the SFP. FDP_ACC.2.1

Application note: operations include reading objects, writing objects, modifying objects, deleting objects, and executing objects by a subject or process operating on behalf of a subject.

5.2.1.2.1.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP. FDP_ACC.2.2

5.2.1.2.2 Security Attribute Based Access Control (FDP_ACF.1)

5.2.1.2.2.1 The TSF shall enforce the [mandatory access control policy] to objects based on [object attributes, subject attributes, environmental attributes, and {*other attributes chosen by the Security Target author*}]. FDP_ACF.1.1

5.2.1.2.2.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: FDP_ACF.1.2

a) [Subject authentication and
b) Access Control List validation

at a minimum, and other rules {*chosen by the Security Target author*}].

5.2.1.2.2.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none]. FDP_ACF.1.3

5.2.1.2.2.4 The TSF shall explicitly deny access of subjects to objects based on the [invalid authentication {*and other rules to be determined by the Security Target author*}]. FDP_ACF.1.4

5.2.1.2.3 Subset Information Flow Control (FDP_IFC.1) (Iteration 1)

5.2.1.2.3.1 The TSF shall enforce the [mandatory access control policy] on [subjects (processes, users, and administrators), information, and operations, except for Community of Interest subjects, information, and operations]. FDP_IFC.1.1(1)

5.2.1.2.4 Subset Information Flow Control (FDP_IFC.1) (Iteration 2)

5.2.1.2.4.1 The TSF shall enforce the [Community of Interest access control policy] on [Community of Interest subjects (processes, users, and administrators), information, and operations]. FDP_IFC.1.1(2)

5.2.1.2.5 Hierarchical Security Attributes (FDP_IFF.2)

5.2.1.2.5.1 The TSF shall enforce the [mandatory access control policy and Community of Interest access control policy] based on the following types of subject and information security attributes: FDP_IFF.2.1

a) [Information attributes;
b) User attributes;
c) Process attributes;
d) Attributes required by an authorized TOE Security Administrator;
e) Community of Interest attributes;
f) {*And other security attributes chosen by the Security Target author*}].

Application note: select attributes based on their ability to enforce the security functional policies. An example of an attribute assigned by a TOE Security Administrator might be a maintainer's user account with restricted permissions.

5.2.1.2.5.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules, based on the ordering relationships between security attributes, hold: [the user or process is authorized by competent authority to have access to the information being requested by the user or process]. FDP_IFF.2.2

5.2.1.2.5.3 The TSF shall enforce the [none]. FDP_IFF.2.3

5.2.1.2.5.4 The TSF shall provide the following: [{*additional capabilities chosen by the Security Target author*}]. FDP_IFF.2.4

5.2.1.2.5.5 The TSF shall explicitly authorize an information flow based on the following rules: [none]. FDP_IFF.2.5

5.2.1.2.5.6 The TSF shall explicitly deny an information flow based on the following rules: [the information is label with a classification label higher that Secret {*and additional rules chosen by the Security Target author*}]. FDP_IFF.2.6

5.2.1.2.5.7 The TSF shall enforce the following relationships for any two valid information flow control security attributes: FDP_IFF.2.7

a) [There exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable;

b) There exists a "least upper bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and

c) There exists a "greatest lower bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is not greater than the two valid security attributes].

5.2.1.2.6 Transmission Separation by Attribute (FDP_ITT.2)

5.2.1.2.6.1 The TSF shall enforce the [mandatory access control policy or the COI access control policy] to prevent the [disclosure, modification, or loss of use] of user data when it is transmitted between physically-separated parts of the TOE. FDP_ITT.2.1

5.2.1.2.6.2 The TSF shall separate data controlled by the SFP(s) when transmitted between physically-separated parts of the TOE, based on the values of the following: [COI membership, role as TOE Security Administrator, role as TOE System Administrator, and {*other attributes chosen by the Security Target author*}]. FDP_ITT.2.2

5.2.1.2.7 Subset Residual Information Protection (FDP_RIP.1)

5.2.1.2.7.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] the following objects: [community of interest objects, objects used to administer TOE security, objects used to administer TOE systems, {*and other objects chosen by the Security Target author*}]. FDP_RIP.1.1

5.2.1.2.8 Basic Data Exchange Confidentiality (FDP_UCT.1)

5.2.1.2.8.1 The TSF shall enforce the [mandatory access control policy and the Community of Interest access control policy] to be able to [transmit and receive] objects in a manner protected from unauthorized disclosure. FDP_UCT.1.1

5.2.1.2.9 Data Exchange Integrity (FDP_UIT.1)

5.2.1.2.9.1 The TSF shall enforce the [mandatory access control policy and the Community of Interest access control policy] to be able to [transmit and receive] user data in a manner protected from [modification, deletion, and insertion] errors. FDP_UIT.1.1

5.2.1.2.9.2 The TSF shall be able to determine on receipt of user data, whether [modification, deletion, or insertion] has occurred. FDP_UIT.1.2

5.2.1.3 Identification and Authentication (FIA)

5.2.1.3.1 Authentication Failure Handling (FIA_AFL.1)

5.2.1.3.1.1 The TSF shall detect when [a single-digit number, which can be preset by a TOE Security Administrator, of] unsuccessful authentication attempts occur related to [reauthentication or login]. FIA_AFL.1.1

Application note: during account creation, the TSF should configure the account to implement the preset number by default.

5.2.1.3.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall FIA_AFL.1.2

a) [If a valid account was specified, lock it and alert all TOE Security Administrators and TOE System Administrators, providing the account identification and reason the TSF took action against the account

b) If an invalid account is specified, disable the terminal].

Application note: an example of disabling the terminal might be breaking off communication from that terminal.

5.2.1.3.2 User Attribute Definition (FIA_ATD.1)

5.2.1.3.2.1 The TSF shall maintain the following list of security attributes belonging to individual users: [identification data, role (user, TOE Security Administrator, TOE System Administrator), Community of Interest membership, nationality, authorization to export information out of the multinational information domain, authorization to receive information imported into the multinational information domain, {*and other user security attributes chosen by the Security Target author*}]. FIA_ATD.1.1

5.2.1.3.3 Verification of Secrets (FIA_SOS.1)

Application note: an example of a secret would be a user password.

5.2.1.3.3.1 The TSF shall provide a mechanism to verify that secrets meet the following criteria: FIA_SOS.1.1

a) [For each attempt to use the mechanism, the probability that a random attempt to provide the correct secret is less than one in 250 trillion (250,000,000,000,000);

Application note: this can be achieved with passwords that contain 8 or more characters (assuming a 63-character alphabet, including at least one numerical and one non-alphabetic character).

b) Any feedback given during a failed authentication attempt will not increase the likelihood that the secret will be discovered;

c) {*And other criteria chosen by the Security Target author*}].

5.2.1.3.4 Timing of Authentication (FIA_UAU.2)

5.2.1.3.4.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. FIA_UAU.2.1

5.2.1.3.5 Re-authenticating (FIA_UAU.6)

5.2.1.3.5.1 The TSF shall re-authenticate the user under the conditions: FIA_UAU.6.1

a) [TSF-initiated session locking has occurred and
b) {*other conditions chosen by the Security Target author*}].

5.2.1.3.6 Protected Authentication Feedback (FIA_UAU.7)

5.2.1.3.6.1 The TSF shall provide only [dummy character feedback] to the user while the authentication is in progress. FIA_UAU.7.1

Application note: typically, the dummy character feedback is an asterisk for each character entered.

5.2.1.3.7 User Identification Before Any Action (FIA_UID.2)

5.2.1.3.7.1 The TSF shall require each user entity to identify itself before allowing any other TSF-mediated actions on behalf of that user. FIA_UID.2.1

5.2.1.3.8 User-Subject Binding (FIA_USB.1)

5.2.1.3.8.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user. FIA_USB.1.1

5.2.1.4 Security Management (FMT)

5.2.1.4.1 Management of Security Functions Behavior (FMT_MOF.1)

5.2.1.4.1.1 The TSF shall restrict the ability to [determine the behavior of, disable, enable, and modify the behavior of] the functions [authentication failure threshold enforcement, user attribute assignment, {*and functions chosen by the Security Target author*}] to [TOE Security Administrators]. FMT_MOF.1.1

Application note: the TOE shall provide user-friendly tools for TOE Security Administrators to perform these functions.

5.2.1.4.2 Management of Security Attributes (FMT_MSA.1) (Iteration 1)

5.2.1.4.2.1 The TSF shall enforce the [mandatory access control policy] to restrict the ability to [change default, query, modify, or delete] the security attributes [TOE Security Administrator, TOE System Administrator, author, releaser, recipient, {*and other attributes chosen by the Security Target author*}] to [TOE Security Administrators]. FMT_MSA.1.1(1)

5.2.1.4.3 Management of Security Attributes (FMT_MSA.1) (Iteration 2)

5.2.1.4.3.1 The TSF shall enforce the [Community of Interest access control policy] to restrict the ability to [modify] the security attributes [object sensitivity label {*and other attributes chosen by the Security Target author*}] to [the author of the object and TOE Security Administrators]. FMT_MSA.1.1(2)

5.2.1.4.4 Secure Security Attributes (FMT_MSA.2)

5.2.1.4.4.1 The TSF shall ensure that only secure values are accepted for security attributes. FMT_MSA.2.1

5.2.1.4.5 Static Attribute Initialization (FMT_MSA.3)

5.2.1.4.5.1 The TSF shall enforce the [mandatory access control policy] to provide [restrictive] default values for security attributes that are used to enforce the SFP. FMT_MSA.3.1

5.2.1.4.5.2 The TSF shall allow the [TOE Security Administrators] to specify alternative initial values to override the default values when an object or information is created. FMT_MSA.3.2

5.2.1.4.6 Management of TSF Data (FMT_MTD.1)

5.2.1.4.6.1 The TSF shall restrict the ability to [change default, query, modify, delete, clear, {*and other operations chosen by the Security Target author*}] the [user attributes, object security attributes, {*and other data chosen by the Security Target author*}] to [TOE Security Administrators]. FMT_MTD.1.1

5.2.1.4.7 Revocation (FMT_REV.1)

5.2.1.4.7.1 The TSF shall restrict the ability to revoke security attributes associated with the [users, subjects, objects, **and cross-domain filtering functions**] within the TSC to [TOE Security Administrators]. FMT_REV.1.1

5.2.1.4.7.2 The TSF shall enforce the rules [prior to the next operation associated with the user, subject, object, or resource]. FMT_REV.1.2

5.2.1.4.8 Restrictions on Security Roles (FMT_SMR.2)

5.2.1.4.8.1 The TSF shall maintain the roles [user, TOE System Administrator, and TOE Security Administrator]. FMT_SMR.2.1

5.2.1.4.8.2 The TSF shall be able to associate users with roles. FMT_SMR.2.2

5.2.1.4.8.3 The TSF shall ensure that the conditions

a) [A user logged in as a TOE Security Administrator cannot simultaneously initiate a session as a TOE System Administrator and

b) A user logged in as a TOE System Administrator cannot simultaneously initiate a session as a TOE Security Administrator]

are satisfied. FMT_SMR.2.3

5.2.1.4.9 Assuming Roles (FMT_SMR.3)

5.2.1.4.9.1 The TSF shall require an explicit request to assume the following roles: [TOE System Administrator and TOE Security Administrator]. FMT_SMR.3.1

5.2.1.5 Protection of TOE Security Functions (FPT)

5.2.1.5.1 Abstract Machine Testing (FPT_AMT.1)

5.2.1.5.1.1 The TSF shall run a suite of tests [during initial start-up, periodically during normal operation, and at the request of an authorized **TOE System Administrator or TOE Security Administrator**] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.[24] FPT_AMT.1.1

5.2.1.5.2 Failure with Preservation of Secure State (FPT_FLS.1)

5.2.1.5.2.1 The TSF shall preserve a secure state when the following types of failures occur: [power failure, detection of a non-secure operation, {*and other failures chosen by the Security Target author*}]. FPT_FLS.1.1

5.2.1.5.3 Notification of Physical Attack (FPT_PHP.2)

5.2.1.5.3.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF. FPT_PHP.2.1

5.2.1.5.3.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred. FPT_PHP.2.2

5.2.1.5.3.3 For [{*TSF devices and elements chosen by the Security Target author*}], the TSF shall monitor the devices and elements and notify [TOE Security and System Administrators] when physical tampering with the TSF's devices or TSF's elements has occurred. FPT_PHP.2.3

Application note: FPT_PHP.1 (Passive Detection of Physical Attack) is acceptable if detection and notification tools are unavailable to implement this requirement.

---

[24] Text was deleted from FPT_AMT.1.1. Rationale: the phrase "user" was replaced with "TOE system administrator or TOE security administrator" to properly define the requirement.

The TSF shall run a suite of tests [at the request of an authorized ~~user~~ TOE system administrator or TOE security administrator] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.2.1.5.4 Automated Recovery (FPT_RCV.2)

5.2.1.5.4.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided. FPT_RCV.2.1

5.2.1.5.4.2 For [electrical power interruption, network communication interruption, {*and other discontinuities chosen by the Security Target author*}], the TSF shall ensure the return of the TOE to a secure state using automated procedures. FPT_RCV.2.2

5.2.1.5.5 Replay Detection (FPT_RPL.1)

5.2.1.5.5.1 The TSF shall detect replay for the following entities: [Access by TOE Administrators *and access by other users specified by authorized TOE Security Administrators*]. FPT_RPL.1.1

5.2.1.5.5.2 The TSF shall ignore the attempted replay operation and generate an audit record when replay is detected. FPT_RPL.1.2

5.2.1.5.6 Non-Bypassability of the TSP (FPT_RVM.1)

5.2.1.5.6.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. FPT_RVM.1.1

5.2.1.5.7 Reliable Time Stamps (FPT_STM.1)

5.2.1.5.7.1 The TSF shall be able to provide reliable time stamps for its own use. FPT_STM.1.1

5.2.1.5.8 Inter-TSF Basic TSF Data Consistency (FPT_TDC.1)

5.2.1.5.8.1 The TSF shall provide the capability to consistently interpret [access control data] when shared between the TSF and another trusted IT product. FPT_TDC.1.1

5.2.1.5.8.2 The TSF shall use [best commercial practices] when interpreting the TSF data from another trusted IT product. FPT_TDC.1.2

5.2.1.5.9 TSF Testing (FPT_TST.1)

5.2.1.5.9.1 The TSF shall run a suite of self-tests [<u>during initial start-up, periodically during normal operation, at the request of</u> **an authorized TOE System Administrator or TOE Security Administrator**, {*and under other conditions chosen by the Security Target author*}] to demonstrate the correct operation of the TSF.[25] FPT_TST.1.1

[25] Text was deleted from FPT_TST.1.1. Rationale: replace the phrase "the authorized user" with "a system administrator or security administrator" to specify that the authorized users are administrators.

> The TSF shall run a suite of self-tests [<u>during initial startup, periodically during normal operation, at the request of</u> ~~the authorized user~~ <u>a system administrator or security administrator</u>, during automatic recovery, {*and other conditions chosen by the Security Target author*}] to demonstrate the correct operation of the TSF. FPT_TST.1.1

5.2.1.5.9.2 The TSF shall provide authorized **TOE Security Administrators** with the capability to verify the integrity of TSF data.[26] FPT_TST.1.2

5.2.1.5.9.3 The TSF shall provide authorized **TOE Security Administrators** with the capability to verify the integrity of stored TSF executable code.[27] FPT_TST.1.3

5.2.1.6 TOE Access (FTA)

5.2.1.6.1 Basic Limitation on Multiple Concurrent Sessions (FTA_MCS.1)

5.2.1.6.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user. FTA_MCS.1.1

5.2.1.6.1.2 The TSF shall enforce, by default, a limit of [a single-digit number, which can be preset by a TOE System Administrator, of] sessions per user. FTA_MCS.1.2

5.2.1.6.2 TSF-Initiated Session Locking (FTA_SSL.1)

5.2.1.6.2.1 The TSF shall lock an interactive session after [a time interval, which can be set by the user, up to a maximum limit configured by an authorized TOE Security Administrator] by: FTA_SSL.1.1

a) Clearing or overwriting display devices, making the current contents unreadable;
b) Disabling any activity of the user's data access/display devices other than unlocking the session.

Application note: the TSF should provide the ability for the TOE Security Administrator to set a default value that is implemented during the creation of each user account. The default value is not required to be equal to the maximum limit and should be less.

5.2.1.6.2.2 The TSF shall require the following events to occur prior to unlocking the session: [user reauthentication, Security Administrator authentication, {*or another event chosen by the Security Target author*}]. FTA_SSL.1.2

---

[26] Text was deleted from FPT_TST.1.2. Rationale: replace the word "users" with the phrase "TOE Security Administrators" to specify that the authorized users are TOE Security Administrators.

The TSF shall provide authorized ~~users~~ TOE Security Administrators with the capability to verify the integrity of TSF data. FPT_TST.1.2

[27] Text was deleted from FPT_TST.1.3. Rationale: replace the word "users" with the phrase "TOE Security Administrators" to specify that the authorized users are TOE Security Administrators.

The TSF shall provide authorized ~~users~~ TOE Security Administrators with the capability to verify the integrity of stored TSF executable code. FPT_TST.1.3

Application note: the TSF will provide the ability for a user or administrator to terminate the session, deactivate the system, or reboot the system if the session cannot be unlocked. Additionally, TOE Security Administrators may enter their authentication credentials (e.g., password) to unlock and resume a user session.

5.2.1.6.3 User-initiated Locking (FTA_SSL.2)

5.2.1.6.3.1 The TSF shall allow user-initiated locking of the user's own interactive session, by: FTA_SSL.2.1

a) Clearing or overwriting display devices, making the current contents unreadable;
b) Disabling any activity of the user's data access/display devices other than unlocking the session.

5.2.1.6.3.2 The TSF shall require the following events to occur prior to unlocking the session: [user reauthentication, TOE Security Administrator authentication, {*or another event chosen by the Security Target author*}]. FTA_SSL.2.2

Application note: the TSF will provide the ability for a user or administrator to terminate the session, deactivate the system, or reboot the system if the session cannot be unlocked. Additionally, TOE Security Administrators may enter their authentication credentials (e.g., password) to unlock and resume a user session.

5.2.1.6.4 TSF-initiated Termination (FTA_SSL.3)

5.2.1.6.4.1 The TSF shall terminate an interactive session after a [time interval of user inactivity, which can be set by an authorized TOE Security Administrator]. FTA_SSL.3.1

5.2.1.6.5 TOE Access History (FTA_TAH.1)

5.2.1.6.5.1 Upon successful session establishment, the TSF shall display the [date, time, and location] of the last successful session establishment to the user. FTA_TAH.1.1

5.2.1.6.5.2 Upon successful session establishment, the TSF shall display the [date, time, and location] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment. FTA_TAH.1.2

5.2.1.6.5.3 The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information. FTA_TAH.1.3

5.2.1.6.6 TOE Session Establishment (FTA_TSE.1)

5.2.1.6.6.1 The TSF shall be able to deny session establishment based on [invalid identification or authentication data]. FTA_TSE.1.1

5.2.2 Cross-Domain Filtering

5.2.2.1 Security Audit (FAU)

5.2.2.1.1 Security Audit Automatic Response (FAU_ARP.1)

5.2.2.1.1.1 The TSF shall [immediately notify TOE Security Administrators and provide a checklist of appropriate responsive actions {as chosen by the Security Target author}] upon detection of a potential security violation.[28] FAU_ARP.1.1

5.2.2.1.2 Audit Data Generation (FAU_GEN.1)

5.2.2.1.2.1 The TSF shall be able to generate an audit record of the following auditable events: FAU_GEN.1.1

d) Start-up and shutdown of the audit functions;
e) All auditable events for the [basic] level of audit;
f) The events in the table (below):

Table 3 - Audit Events for Cross-Domain Filtering

Functional Component	Auditable Event	Additional Audit Record Contents (beyond those in FAU_GEN.1.2)
FAU_ARP.1	Detection of a potential security violation.	The identifier of the potential security violation.
FAU_SAA.2	Creating, modifying, or changing the internal representation of any of the signature events. Enabling or disabling the comparison of any of the signature events.	The identity of the authorized administrator performing the operation. The system event that occurs when it matches a signature event.
FAU_SAA.3	Creating, modifying, or changing the internal representation of any of the signature events. Enabling or disabling the comparison of any of the signature events.	The identity of the authorized administrator performing the operation. The system event that occurs when it matches a signature event.

[28] Text was deleted from FAU_ARP.1.1. Rationale: the word "take" was deleted for better textual flow of the requirement.

The TSF shall ~~take~~ [immediately notify security administrators and provide a checklist of appropriate responsive actions {*as chosen by the Security Target author*}] upon detection of a potential security violation. FAU_ARP.1.1

Functional Component	Auditable Event	Additional Audit Record Contents (beyond those in FAU_GEN.1.2)
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	The identity of the administrator performing the modification and the prior configuration of any excluded audit events.
FCO_NRO.1	The invocation of the non-repudiation service.	The identity of the originator, the destination, and a copy of the non-repudiation evidence for the information being transferred.
FDP_ACC.2	All requests to perform an operation by a subject or on an object covered by the policy.	The identity of the subject requesting the operation and the identity of the object.
FDP_ACF.1	All requests to perform an operation on an object covered by the policy.	The identity of the subject requesting the operation and the identity of the object, and, if access was denied, the reason the TSF denied access.
FDP_DAU.1	Unsuccessful generation of validity evidence.	The identity of the subject that created the information and the reason the information is considered invalid.
FDP_ETC.2	All attempts to export information.	The address of the presumed sender and recipient(s) and a copy of the information object being exported.
FDP_IFC.2	(None)	(None)
FDP_IFF.2	All decisions on requests for information flow.	The address of the presumed sender and recipient(s), and, if the information flow was denied, the reason the TSF denied it.
FDP_IFF.3	All decisions on requests for information flow. The use of identified illicit information flow channels.	The address of the presumed sender and recipient(s), the reason the flow was determined to be illicit, and the channel used by the illicit flow.
FDP_ITC.2	All attempts to import user data including any security attributes.	The address of the presumed sender and recipient(s) and, if the TOE blocked the importation of the data, a copy of the rejected data and the reason for rejection.
FDP_RIP.2	(None)	(None)
FIA_AFL.1	Reaching the threshold for unsuccessful authentication attempts and the actions taken, and the subsequent restoration to normal operational state.	The identity of the offending user and the identity of the administrator that restored the system to normal operation.
FIA_ATD.1	(None)	(None)

Functional Component	Auditable Event	Additional Audit Record Contents (beyond those in FAU_GEN.1.2)
FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret.	The identity of the user and the feedback information provided.
FIA_UAU.2	All use of the authentication mechanism.	The user identities being presented.
FIA_UID.2	All use of the user identification mechanism, including the user identity provided.	The user identities being presented.
FIA_USB.1	Success or failure of binding of user security attributes to a subject (such as success or failure to create a subject).	The subject identity, the security attribute(s), and the binding result.
FMT_MOF.1	All modifications in the behavior of the functions in the TSF.	The identity of the administrator performing the modification.
FMT_MSA.1	All modifications of the values of security attributes.	The identity of the administrator performing the modification.
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules and all modifications of the initial values of security attributes.	The identity of the administrator performing the modification.
FMT_MTD.1	All modifications to the values of TSF data.	The identity of the administrator performing the modification and the before and after values of the changed data.
FMT_SMR.1	Modifications to the group of users that are part of a role.	The identity of the administrator performing the modification.
FMT_SMR.3	Explicit request to assume a role.	The identity of the user making the request.
FPT_AMT.1	Execution of the tests of the underlying machine and the results of the tests.	The identity of the administrator performing the operation.
FPT_FLS.1	Failure of the TSF.	The identity of the failed mechanism(s) and the reason for failure, if discernable.
FPT_ITT.1	(None)	(None)
FPT_RCV.2	Type of failure or service discontinuity.	Whether automatic recovery was successful or not and reason for inability to automatically recover, if discernable.
FPT_RVM.1	(None)	(None)
FPT_SEP.3	(None)	(None)
FPT_STM.1	Changes to the time.	The identity of the administrator changing the time.

Functional Component	Auditable Event	Additional Audit Record Contents (beyond those in FAU_GEN.1.2)
FPT_TDC.1	Use of the TSF data consistency mechanisms, identification of which TSF data have been interpreted, and detection of modified TSF data.	The address of the presumed source and destination(s).
FPT_TST.1	Execution of the TSF self tests and the results of the test.	The reason for execution of the test(s) and, when requested by an authorized administrator, the identity of the administrator.
FRU_FLT.1	Any failure detected by the TSF.	The failure type.
FRU_RSA.1	All attempted uses of the resource allocation functions for resources that are under control of the TSF.	The identity of users who reach the quota and the identifier of the quota that was reached.
FTP_TRP.1	All attempted uses of the trusted path functions and identification of the user associated with all trusted path invocations.	The identity of users who initiate communication via a trusted path.

5.2.2.1.2.2 The TSF shall record within each audit record at least the following information: FAU_GEN.1.2

c) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
d) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST:
   – [The sensitivity label attached to applicable objects,
   – The before and after value(s) of changed configuration settings, lists, or tables,
   – {*And other user attributes and data chosen by the Security Target author*}]

5.2.2.1.3 Profile Based Anomaly Detection (FAU_SAA.2)

5.2.2.1.3.1 The TSF shall be able to maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the member(s) of [partner nations, communities of interest, all users, all administrators, groups identified by a TOE Security Administrator, {*and groups chosen by the Security Target author*}]. FAU_SAA.2.1

5.2.2.1.3.2 The TSF shall be able to maintain a suspicion rating associated with each user whose activity is recorded in a profile, where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile. FAU_SAA.2.2

5.2.2.1.3.3 The TSF shall be able to indicate an imminent violation of the TSP when a user's suspicion rating exceeds the following threshold conditions [maximum cross-domain file transfer rate, maximum size of a file being transferred across the domain boundary, {*and other thresholds chosen and configured by a TOE Security Administrator*}]. FAU_SAA.2.3

5.2.2.1.4 Simple Attack Heuristics (FAU_SAA.3)

5.2.2.1.4.1 The TSF shall be able to maintain an internal representation of the following signature events [accumulation or combination of invalid authentication attempts, user attempt to access system files, {*and other events chosen by the Security Target author*}] that may indicate a violation of the TSP. FAU_SAA.3.1

Application note: "system files" might include audit records, user attribute files, password files, etc.

5.2.2.1.4.2 The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of [TOE component audit files {*and other records chosen by the Security Target author*}]. FAU_SAA.3.2

5.2.2.1.4.3 The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP. FAU_SAA.3.3

5.2.2.1.5 Selective Audit (FAU_SEL.1)

5.2.2.1.5.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes: FAU_SEL.1.1

a) [Host identity and event type]
b) [*Attributes included by an authorized TOE Security Administrator*].

Application note: the intent of split administration is to prohibit an administrator from individually performing certain actions. One of these prohibited actions is the ability for an individual to exclude auditable events. There is no intent to require the TOE to store audit records; the TOE will send audit records to an audit storage and analysis capability in the TSE.

5.2.2.2 Communication (FCO)

5.2.2.2.1 Selective Proof of Origin (FCO_NRO.1)

5.2.2.2.1.1 The TSF shall be able to generate evidence of origin for transmitted [information that is destined to cross an information domain boundary] at the request of the [inter-domain transfer process]. FCO_NRO.1.1

5.2.2.2.1.2 The TSF shall be able to relate the [identity {*and other attributes chosen by the Security Target author*}] of the originator of the information, and the [content and time and date of origin] of the information to which the evidence applies. FCO_NRO.1.2

5.2.2.2.1.3 The TSF shall provide a capability to verify the evidence of origin of information to [the TOE Security Administrator and TOE System Administrator] given [a certification infrastructure and individual certificates]. FCO_NRO.1.3

5.2.2.3 User Data Protection (FDP)

5.2.2.3.1 Complete Access Control (FDP_ACC.2)

5.2.2.3.1.1 The TSF shall enforce the [mandatory access control policy] on [subjects and objects that interact with cross-domain transfer processes] and all operations among subjects and objects covered by the SFP. FDP_ACC.2.1

5.2.2.3.1.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP. FDP_ACC.2.2

5.2.2.3.2 Security Attribute Based Access Control (FDP_ACF.1)

5.2.2.3.2.1 The TSF shall enforce the [mandatory access control policy] to objects based on [object attributes, subject attributes, environmental attributes, and {*other attributes chosen by the Security Target author*}]. FDP_ACF.1.1

5.2.2.3.2.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [{*chosen by the Security Target author}*]. FDP_ACF.1.2

5.2.2.3.2.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [valid digital signatures {*or an authentication approach chosen by the Security Target author to be equivalent*} will be required to authenticate the subject associated with network transmissions]. FDP_ACF.1.3

5.2.2.3.2.4 The TSF shall explicitly deny access of subjects to objects based on the [invalid user certificate, invalid subject authentication, {*and other rules to be determined by the Security Target author*}]. FDP_ACF.1.4

5.2.2.3.3 Basic Data Authentication (FDP_DAU.1)

5.2.2.3.3.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [information that is destined to cross an information domain boundary, information used by the TSF to enforce security policies, and {*other objects or information chosen by the Security Target author*}]. FDP_DAU.1.1

5.2.2.3.3.2 The TSF shall provide [cross-domain transfer processes and TOE Security Administrators] with the ability to verify evidence of the validity of the indicated information. FDP_DAU.1.2

5.2.2.3.4 Export of User Data with Security Attributes (FDP_ETC.2)

5.2.2.3.4.1 The TSF shall enforce the [cross-domain transfer policy] when exporting user data, controlled under the SFP(s), outside of the TSC. FDP_ETC.2.1

5.2.2.3.4.2 The TSF shall export the user data with the user data's associated security attributes. FDP_ETC.2.2

5.2.2.3.4.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data. FDP_ETC.2.3

5.2.2.3.4.4 The TSF shall enforce the following rules when user data is exported from the TSC: [{*chosen by the Security Target author}*]. FDP_ETC.2.4

5.2.2.3.5 Complete Information Flow Control (FDP_IFC.2)

5.2.2.3.5.1 The TSF shall enforce the [cross-domain transfer policy] on [subjects (processes, users, and administrators), information (that may cross the multinational information domain boundary), and operations (that cause information to be transferred across the multinational information domain boundary)] and all operations that cause that information to flow to and from subjects covered by the SFP. FDP_IFC.2.1

5.2.2.3.5.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP. FDP_IFC.2.2

5.2.2.3.6 Hierarchical Security Attributes (FDP_IFF.2)

5.2.2.3.6.1 The TSF shall enforce the [mandatory access control and cross-domain transfer policies] based on the following types of subject and information security attributes: FDP_IFF.2.1

g) [Information type, sensitivity, and originator;
h) Destination domain security authorization and protections;
i) Sender authorizations;
j) Recipient authorizations;
k) Attributes required by an authorized TOE Security Administrator;
l) {*And other security attributes chosen by the Security Target author*}].

Application note: select attributes based on their ability to enforce the security functional policies.

5.2.2.3.6.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules, based on the ordering relationships between security attributes hold: FDP_IFF.2.2

a) [The information flow must comply with the cross-domain transfer policy and
b) The inter-domain transfer process must validate and regrade the information in compliance with the cross-domain transfer policy before transferring it from one information domain to another].

5.2.2.3.6.3 The TSF shall enforce the [policies implemented by an authorized TOE Security Administrator]. FDP_IFF.2.3

5.2.2.3.6.4 The TSF shall provide the following: [stop list check capability {*and additional security filters chosen by the Security Target author*}]. FDP_IFF.2.4

Application note: the stop list is sometimes called a "dirty word" list

5.2.2.3.6.5 The TSF shall explicitly authorize an information flow based on the following rules: [none]. FDP_IFF.2.5

5.2.2.3.6.6 The TSF shall explicitly deny an information flow based on the following rules: FDP_IFF.2.6

a) [Information that contains malicious content,
b) Information that is not in an authorized format,
c) Information that contains unauthorized or ambiguous content,
d) Information transferred by an unauthorized protocol,
e) Information classified higher than Secret,
f) Information sent by an unauthorized person or process,
g) Information sent to an unauthorized person or process,
h) Rules specified by an authorized TOE Security Administrator,
i) {*And additional rules chosen by the Security Target author*}].

5.2.2.3.6.7 The TSF shall enforce the following relationships for any two valid information flow control security attributes: FDP_IFF.2.7

a) There exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable; and
b) There exists a "least upper bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and
c) There exists a "greatest lower bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is not greater than the two valid security attributes.

5.2.2.3.7 Limited Illicit Information Flows (FDP_IFF.3)

5.2.2.3.7.1 The TSF shall enforce the [cross-domain transfer policy] to limit the capacity of [unauthorized information to leak or covertly be transferred across the information domain boundary] to a [{*capacity chosen by the Security Target author*}]. FDP_IFF.3.1

5.2.2.3.8 Import of User Data with Security Attributes (FDP_ITC.2)

5.2.2.3.8.1 The TSF shall enforce the [cross-domain transfer policy] when importing user data, controlled under the SFP, from outside of the TSC. FDP_ITC.2.1

5.2.2.3.8.2 The TSF shall use the security attributes associated with the imported user data. FDP_ITC.2.2

5.2.2.3.8.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received. FDP_ITC.2.3

5.2.2.3.8.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data. FDP_ITC.2.4

5.2.2.3.8.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [the data must not contain known malicious content and the import of data must comply with the cross-domain transfer policy, otherwise the TOE shall not import the data]. FDP_ITC.2.5

5.2.2.3.9 Full Residual Information Protection (FDP_RIP.2)

5.2.2.3.9.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [allocation of the resource to and the deallocation of the resource from] all objects. FDP_RIP.2.1

5.2.2.4 Identification and Authentication (FIA)

5.2.2.4.1 Authentication Failure Handling (FIA_AFL.1)

5.2.2.4.1.1 The TSF shall detect when [a single-digit number, which can be preset by a TOE Security Administrator, of] unsuccessful authentication attempts occur related to [reauthentication or login]. FIA_AFL.1.1

5.2.2.4.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [perform actions pre-specified by the TOE Security Administrator, such as disabling the account until unlocked by a TOE Security Administrator {*or other actions chosen by the Security Target author*} and alert all TOE Security Administrators and TOE System Administrators, providing the account information and reason the TSF took action against the account]. FIA_AFL.1.2

Application note: an example of a pre-specified action would be for the TSF to lock the account from user access after a specified number of unsuccessful authentication attempts.

5.2.2.4.2 User Attribute Definition (FIA_ATD.1)

5.2.2.4.2.1 The TSF shall maintain the following list of security attributes belonging to individual users: [authentication data, role, group membership, nationality, authorization to export information out of the multinational information domain, authorization to receive information imported into the multinational information domain, {*and other user security attributes chosen by the Security Target author*}]. FIA_ATD.1.1

5.2.2.4.3 Verification of Secrets (FIA_SOS.1)

5.2.2.4.3.1 The TSF shall provide a mechanism to verify that secrets meet **the following criteria**: FIA_SOS.1.1

a) [For each attempt to use the mechanism, the probability that a random attempt to provide the correct secret is less than one in 250 trillion (250,000,000,000,000);

Application note: this can be achieved with passwords that contain 8 or more characters (assuming a 63-character alphabet, including at least one numerical and one non-alphabetic character).

b) Any feedback given during a failed authentication attempt will not increase the likelihood that the secret will be discovered;

c) {*And other criteria chosen by the Security Target author*}].

5.2.2.4.4 Timing of Authentication (FIA_UAU.2)

5.2.2.4.4.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. FIA_UAU.2.1

5.2.2.4.5 User Identification Before Any Action (FIA_UID.2)

5.2.2.4.5.1 The TSF shall require each user entity to identify itself before allowing any other TSF-mediated actions on behalf of that user. FIA_UID.2.1

5.2.2.4.6 User-Subject Binding (FIA_USB.1)

5.2.2.4.6.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user. FIA_USB.1.1

5.2.2.5 Security Management (FMT)

5.2.2.5.1 Management of Security Functions Behavior (FMT_MOF.1)

5.2.2.5.1.1 The TSF shall restrict the ability to [<u>determine the behavior of, disable, enable, and modify the behavior of</u>] the functions [of audit, authentication failure thresholds, user attribute assignment, {*and functions chosen by the Security Target author*}] to [TOE Security Administrators]. FMT_MOF.1.1

Application note: the TOE shall provide user-friendly tools for TOE Security Administrators to perform these functions.

5.2.2.5.2 Management of Security Attributes (FMT_MSA.1)

5.2.2.5.2.1 The TSF shall enforce the [security administration policy] to restrict the ability to [<u>change default, query, modify, or delete</u>] the security attributes [administrator, author, releaser, recipient, sensitivity label, {*and other attributes chosen by the Security Target author*}] to [TOE Security Administrators]. FMT_MSA.1.1

5.2.2.5.3 Static Attribute Initialization (FMT_MSA.3)

5.2.2.5.3.1 The TSF shall enforce the [security administration policy] to provide [restrictive] default values for security attributes that are used to enforce the SFP. FMT_MSA.3.1

5.2.2.5.3.2 The TSF shall allow the [TOE Security Administrators] to specify alternative initial values to override the default values when an object or information is created. FMT_MSA.3.2

5.2.2.5.4 Management of TSF Data (FMT_MTD.1)

5.2.2.5.4.1 FMT_MTD.1.1 The TSF shall restrict the ability to [query] the [audit data, and {*other data chosen by the Security Target author*}] to [TOE Security and System Administrators].

Application note: the TOE shall prevent any user or administrator from modifying the audit data. The audit data will not be deleted until it has been properly reviewed and archived in the TOE security environment.

5.2.2.5.5 Security Roles (FMT_SMR.1)

5.2.2.5.5.1 The TSF shall maintain the roles [TOE System Administrator and TOE Security Administrator]. FMT_SMR.1.1

5.2.2.5.5.2 The TSF shall be able to associate users with roles. FMT_SMR.1.2

5.2.2.5.6 Assuming Roles (FMT_SMR.3)

5.2.2.5.6.1 The TSF shall require an explicit request to assume the following roles: [TOE System Administrator and TOE Security Administrator]. FMT_SMR.3.1

5.2.2.6 Protection of TOE Security Functions (FPT)

5.2.2.6.1 Abstract Machine Testing (FPT_AMT.1)

5.2.2.6.1.1 The TSF shall run a suite of tests [during initial startup, during automatic recovery, and at the request of a TOE System Administrator or TOE Security Administrator] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF. FPT_AMT.1.1

5.2.2.6.2 Failure with Preservation of Secure State (FPT_FLS.1)

5.2.2.6.2.1 The TSF shall preserve a secure state when the following types of failures occur: [failure of any cross-domain policy enforcement mechanism, power failure, and {*other failures chosen by the Security Target author*}]. FPT_FLS.1.1

5.2.2.6.3 FPT_ITT.1 Basic internal TSF data transfer protection

5.2.2.6.3.1 The TSF shall protect TSF data from [modification] when it is transmitted between separate parts of the TOE. FPT_ITT.1.1

Application note: virus signature file transfer is one example of an internal TSF data transfer.

5.2.2.6.4 Automated Recovery (FPT_RCV.2)

5.2.2.6.4.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided. FPT_RCV.2.1

5.2.2.6.4.2 For [electrical power interruption, network communication interruption, and {*other discontinuities chosen by the Security Target author*}], the TSF shall ensure the return of the TOE to a secure state using automated procedures. FPT_RCV.2.2

5.2.2.6.5 Non-Bypassability of the TSP (FPT_RVM.1)

5.2.2.6.5.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. FPT_RVM.1.1

5.2.2.6.6 Complete Reference Monitor (FPT_SEP.3)

5.2.2.6.6.1 The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. FPT_SEP.3.1

5.2.2.6.6.2 The TSF shall enforce separation between the security domains of subjects in the TSC. FPT_SEP.3.2

5.2.2.6.6.3 The TSF shall maintain the part of the TSF that enforces the access control and/or information flow control SFPs in a security domain for its own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to the TSP. FPT_SEP.3.3

5.2.2.6.7 Reliable Time Stamps (FPT_STM.1)

5.2.2.6.7.1 The TSF shall be able to provide reliable time stamps for its own use. FPT_STM.1.1

5.2.2.6.8 Inter-TSF Basic TSF Data Consistency (FPT_TDC.1)

5.2.2.6.8.1 The TSF shall provide the capability to consistently interpret [objects and their security attributes] when shared between the TSF and another trusted IT product. FPT_TDC.1.1

5.2.2.6.8.2 The TSF shall use [rules {*chosen by the Security Target author*}] when interpreting the TSF data from another trusted IT product. FPT_TDC.1.2

Application note: virus signature file transfer is one example of an internal TSF data transfer.

5.2.2.6.9 TSF Testing (FPT_TST.1)

5.2.2.6.9.1 The TSF shall run a suite of self-tests [during initial startup, periodically during normal operation, at the request of a TOE System Administrator or TOE Security Administrator, during automatic recovery, {*and other conditions chosen by the Security Target author*}] to demonstrate the correct operation of the TSF.[29] FPT_TST.1.1

5.2.2.6.9.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data. FPT_TST.1.2

5.2.2.6.9.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code. FPT_TST.1.3

5.2.2.7 Resource Utilization (FRU)

5.2.2.7.1 Degraded Fault Tolerance (FRU_FLT.1)

5.2.2.7.1.1 The TSF shall [save all files being processed, if possible and fail safe] when the following failures occur: [loss of power or network connection, hardware failure, or software failure].[30] FRU_FLT.1.1

Application note: if secure degraded operation is possible, such as during the loss of a network connection, then the TOE is not required to enter a fail safe mode.

5.2.2.7.2 Maximum Quotas (FRU_RSA.1)

5.2.2.7.2.1 The TSF shall enforce maximum quotas of the following resources: [total throughput capacity of the cross-domain transfer processes] that [**an** individual user] can use [over a TOE Security Administrator-specified period of time]. FRU_RSA.1.1

---

[29] Text was deleted from FPT_TST.1.1. Rationale: replace the phrase "the authorized user" with "a system administrator or security administrator" to specify that the authorized users are administrators.

> The TSF shall run a suite of self-tests [during initial startup, periodically during normal operation, at the request of ~~the authorized user~~ a system administrator or security administrator, during automatic recovery, {*and other conditions chosen by the Security Target author*}] to demonstrate the correct operation of the TSF. FPT_TST.1.1

[30] Text was deleted from FRU_FLT.1.1. Rationale: the phrase "ensure the operation of" was deleted for better textual flow of the requirement.

> The TSF shall ~~ensure the operation of~~ [save all files being processed, if possible and fail safe] when the following failures occur: [loss of power or network connection, hardware failure, or software failure]. FRU_FLT.1.1

5.2.2.8 Trusted Path/Channels (FTP)

5.2.2.8.1 Trusted Path (FTP_TRP.1)

5.2.2.8.1.1 The TSF shall provide a communication path between itself and [remote and local **TOE Security Administrators and TOE System Administrators**] that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure. FTP_TRP.1.1

5.2.2.8.1.2 The TSF shall permit [local and remote **TOE Security Administrators and TOE System Administrators**] to initiate communication via the trusted path. FTP_TRP.1.2

5.2.2.8.1.3 The TSF shall require the use of the trusted path for [initial authentication **of TOE Security Administrators and TOE System Administrators**, software installation, management of the cross-domain process, {*and for other services chosen by the Security Target author*}]. FTP_TRP.1.3

5.2.3 Security Administration

5.2.3.1 Security Audit (FAU)

5.2.3.1.1 Security Audit Automatic Response (FAU_ARP.1)

5.2.3.1.1.1 The TSF shall take [appropriate responsive actions {*as chosen by the Security Target author*}] upon detection of a potential security violation. FAU_ARP.1.1

5.2.3.1.2 Audit Data Generation (FAU_GEN.1)

5.2.3.1.2.1 The TSF shall be able to generate an audit record of the following auditable events: FAU_GEN.1.1

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [basic] level of audit;
c) The events in the table (below):

Table 4 - Audit Events for Security Administration

Functional Component	Auditable Event	Additional Audit Record Contents (beyond those in FAU_GEN.1.2)
FAU_ARP.1	Detection of a potential security violation.	The identifier of the potential security violation.
FAU_SAA.2	Creating, modifying, or changing the internal representation of any of the signature events. Enabling or disabling the comparison of any of the signature events.	The name of the signature event. The system event that occurs when it matches a signature event.
FAU_SAA.3	Creating, modifying, or changing the internal representation of any of the signature events. Enabling or disabling the comparison of any of the signature events.	The name of the signature event. The system event that occurs when it matches a signature event.
FAU_SAR.1	Reading of information from the audit records.	(None)
FAU_SAR.2	Unsuccessful attempts to read of information from the audit records.	Reason for failure.
FAU_SAR.3	(None)	(None)
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	(None)

Functional Component	Auditable Event	Additional Audit Record Contents (beyond those in FAU_GEN.1.2)
FCO_NRO.1	The invocation of the non-repudiation service.	The identity of the originator, the destination, and a copy of the non-repudiation evidence for the information being transferred.
FDP_ACC.2	All requests to perform an operation by a subject or on an object covered by the policy.	If access was denied, the reason the TSF blocked the operation.
FDP_ACF.1	All requests to perform an operation on an object covered by the policy.	If access was denied, the reason the TSF blocked the operation.
FDP_DAU.1	Unsuccessful generation of validity evidence.	The identity of the subject that created the information and the reason the information is considered invalid.
FDP_IFC.2	(None)	(None)
FDP_IFF.1	All decisions on requests for information flow.	The address of the presumed sender and recipient(s), and, if the information flow was denied, the reason the TSF denied it.
FDP_RIP.1	(None)	(None)
FDP_ROL.1	All attempts to perform rollback operations.	The outcome of the rollback attempt.
FIA_AFL.1	Reaching the threshold for unsuccessful authentication attempts and the actions taken, and the subsequent restoration to normal operational state.	The identity being presented, the identity of the terminal or communication channel, and the identity of the administrator that restored the system to normal operation.
FIA_ATD.1	(None)	(None)
FIA_UAU.2	All use of the authentication mechanism.	The user identity being presented.
FIA_UAU.5	All use of the multiple authentication mechanism.	The user identity being presented, the result of each activated mechanism, and the final decision.
FIA_UAU.6	All reauthentication attempts.	(None)
FIA_UID.2	All use of the user identification mechanism, including the user identity provided.	The user identity being presented.
FIA_USB.1	Success or failure of binding of user security attributes to a subject (such as success or failure to create a subject).	The subject identity, the security attribute(s), and the binding result.
FMT_MOF.1	All modifications in the behavior of the functions in the TSF.	(None)

Functional Component	Auditable Event	Additional Audit Record Contents (beyond those in FAU_GEN.1.2)
FMT_MSA.2	All offered and rejected values for a security attribute.	The value being offered and reason for rejection.
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules and all modifications of the initial values of security attributes.	(None)
FMT_MTD.1	All modifications to the values of TSF data.	The identity of the administrator performing the modification and the before and after values of the changed data.
FMT_MTD.2	All modifications to the limits of TSF data and all modifications to the actions to be taken in case of violation of the limits.	(None)
FMT_MTD.3	All rejected values of TSF data.	Reason for rejection.
FMT_REV.1	All attempts to revoke security attributes.	(None)
FMT_SMR.2	Modifications to the group of users that are part of a role. Unsuccessful attempts to use a role due to the given conditions on the roles.	Reason for failure to use the role.
FMT_SMR.3	Explicit request to assume a role.	(None)
FPR_UNO.4	The observation of the use of a resource or service by a user or subject.	The resource or service being observed and the identity of the subject using the resource or service.
FPT_AMT.1	Execution of the tests of the underlying machine and the results of the tests.	Reason the test execution cannot be completed.
FPT_FLS.1	Failure of the TSF.	The identity of the failed mechanism(s) and the reason for failure, if discernable.
FPT_ITI.1	Detection of modification of transmitted data.	Reason for detection and the action taken in response.
FPT_ITT.1	(None)	(None)
FPT_ITT.3	Detection of an integrity error.	Reason for detection and the action taken in response.
FPT_PHP.2	Detection of tampering.	Reason for detection and action taken in response.
FPT_RCV.2	Type of failure or service discontinuity.	Whether automatic recovery was successful or not and reason for inability to automatically recover, if discernable.
FPT_SEP.1	(None)	(None)

Functional Component	Auditable Event	Additional Audit Record Contents (beyond those in FAU_GEN.1.2)
FPT_STM.1	Changes to the time.	(None)
FPT_TST.1	Execution of the TSF self tests and the results of the test.	The reason for execution of the test(s) and the test results.
FRU_FLT.1	Any failure detected by the TSF.	The failure type and the action taken by the TSF.
FTA_MCS.2	Rejection of a new session based on the limitation of multiple concurrent sessions.	(None)
FTA_SSL.1	Any attempts at unlocking an interactive session.	The approach taken to unlock the session if the user was unsuccessful in unlocking the session normally.
FTA_SSL.2	Any attempts at unlocking an interactive session.	The approach taken to unlock the session if the user was unsuccessful in unlocking the session normally.
FTA_TAB.1	(None)	(None)
FTP_ITC.1	All attempted uses of the trusted channel functions and identification of the initiator and target of all trusted channel functions.	(None)

5.2.3.1.2.2 The TSF shall record within each audit record at least the following information: FAU_GEN.1.2

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST:
   - [The sensitivity label attached to applicable objects,
   - The before and after value(s) of changed configuration settings, lists, or tables,
   - The identity of the user or administrator who made the change,
   - {*And other user attributes and data chosen by the Security Target author*}]

5.2.3.1.3 User Identity Association (FAU_GEN.2)

5.2.3.1.3.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event. FAU_GEN.2.1

5.2.3.1.4 Profile Based Anomaly Detection (FAU_SAA.2)

5.2.3.1.4.1 The TSF shall be able to maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the member(s) of

[partner nations, Communities of Interest, users, TOE Administrators, groups identified by a TOE Security Administrator, {*and groups chosen by the Security Target author*}]. FAU_SAA.2.1

5.2.3.1.4.2 The TSF shall be able to maintain a suspicion rating associated with each user whose activity is recorded in a profile, where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile. FAU_SAA.2.2

5.2.3.1.4.3 The TSF shall be able to indicate an imminent violation of the TSP when a user's suspicion rating exceeds the following threshold conditions [{*to be chosen by the Security Target author and configured by the TOE Security Administrator*}]. FAU_SAA.2.3

5.2.3.1.5 Simple Attack Heuristics (FAU_SAA.3)

5.2.3.1.5.1 The TSF shall be able to maintain an internal representation of the following signature events [accumulation or combination of invalid authentication attempts, user attempt to access system or security files, user attempt to gain access to unauthorized user files, {*and other events chosen by the Security Target author*}] that may indicate a violation of the TSP. FAU_SAA.3.1

5.2.3.1.5.2 The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of [TOE component audit files {*and other records chosen by the Security Target author*}]. FAU_SAA.3.2

5.2.3.1.5.3 The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP. FAU_SAA.3.3

5.2.3.1.6 Audit Review (FAU_SAR.1)

5.2.3.1.6.1 The TSF shall provide [TOE Security and System Administrators] with the capability to read [all audit information] from the audit records. FAU_SAR.1.1

5.2.3.1.6.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information. FAU_SAR.1.2

5.2.3.1.7 Restricted Audit Review (FAU_SAR.2)

5.2.3.1.7.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. FAU_SAR.2.1

5.2.3.1.8 Selectable Audit Review (FAU_SAR.3)

5.2.3.1.8.1 The TSF shall provide the ability to perform [searches and sorting] of audit data based on [user identity, date, time, role, partner nation, community of interest, {*and other criteria chosen by the Security Target author*}]. FAU_SAR.3.1

5.2.3.1.9 Selective Audit (FAU_SEL.1)

5.2.3.1.9.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes: FAU_SEL.1.1

a) [Host identity and event type]
b) [*Attributes included by an authorized TOE Security Administrator*].

Application note: the intent of split administration is to prohibit an administrator from individually performing certain actions. One of these prohibited actions is the ability for one individual to exclude auditable events. There is no intent to require the TOE to store audit records; the TOE will send audit records to an audit storage and analysis capability in the TSE.

5.2.3.2 Communication (FCO)

5.2.3.2.1 Selective Proof of Origin (FCO_NRO.1)

5.2.3.2.1.1 The TSF shall be able to generate evidence of origin for transmitted [administrative commands] at the request of the [TOE administrative processes that receive the commands]. FCO_NRO.1.1

5.2.3.2.1.2 The TSF shall be able to relate the [identity] of the originator of the information, and the [command content] of the information to which the evidence applies. FCO_NRO.1.2

5.2.3.2.1.3 The TSF shall provide a capability to verify the evidence of origin of information to [TOE administrative processes that receive the commands] given [that verification must occur prior to implementing the administrative commands]. FCO_NRO.1.3

Application note: this security requirement (FCO_NRO.1) is intended to apply to remote administration of the TOE and is not required when the TOE is administered locally.

5.2.3.3 User Data Protection (FDP)

5.2.3.3.1 Complete Access Control (FDP_ACC.2)

5.2.3.3.1.1 The TSF shall enforce the [mandatory access control policy] on [subjects and objects] and all operations among subjects and objects covered by the SFP. FDP_ACC.2.1

5.2.3.3.1.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP. FDP_ACC.2.2

5.2.3.3.2 Security Attribute Based Access Control (FDP_ACF.1)

5.2.3.3.2.1 The TSF shall enforce the [mandatory access control policy] to objects based on [object attributes, subject attributes, environmental attributes, and {*other attributes chosen by the Security Target author*}]. FDP_ACF.1.1

5.2.3.3.2.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [{*chosen by the Security Target author}*]. FDP_ACF.1.2

5.2.3.3.2.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none]. FDP_ACF.1.3

5.2.3.3.2.4 The TSF shall explicitly deny access of subjects to objects based on the [invalid authentication {*and other rules to be determined by the Security Target author*}]. FDP_ACF.1.4

5.2.3.3.3 Basic Data Authentication (FDP_DAU.1)

5.2.3.3.3.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [objects or information used to enforce system security {*and other objects or information chosen by the Security Target author*}]. FDP_DAU.1.1

5.2.3.3.3.2 The TSF shall provide [TOE Security and System Administrators] with the ability to verify evidence of the validity of the indicated information. FDP_DAU.1.2

5.2.3.3.4 Complete Information Flow Control (FDP_IFC.2) (Iteration 1)

5.2.3.3.4.1 The TSF shall enforce the [mandatory access control policy] on [subjects (processes, users, and administrators) and information] and all operations that cause that information to flow to and from subjects covered by the SFP. FDP_IFC.2.1(1)

5.2.3.3.4.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP. FDP_IFC.2.2(1)

5.2.3.3.5 Complete Information Flow Control (FDP_IFC.2) (Iteration 2)

5.2.3.3.5.1 The TSF shall enforce the [cross-domain transfer policy] on [subjects (processes, users, and administrators), information that will cross an information domain boundary, and operations that cause information to be transferred across an information domain boundary] and all operations that cause that information to flow to and from subjects covered by the SFP. FDP_IFC.2.1(2)

5.2.3.3.5.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP. FDP_IFC.2.2(2)

5.2.3.3.6 Simple Security Attributes (FDP_IFF.1)

5.2.3.3.6.1 The TSF shall enforce the [mandatory access control and cross-domain transfer policies] based on the following types of subject and information security attributes: FDP_IFF.1.1

a) [Information attributes;
b) User attributes;
c) Process attributes;
d) Attributes required by an authorized TOE Security Administrator;
e) Community of Interest attributes;
f) {*And other security attributes chosen by the Security Target author*}].

Application note: select attributes based on their ability to enforce the security functional policies.

5.2.3.3.6.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [the user or process is authorized by competent authority to have access to the information being requested by the user or process {*and other rules chosen by the Security Target author*}]. FDP_IFF.1.2

5.2.3.3.6.3 The TSF shall enforce the [*additional rules implemented by an authorized TOE Security Administrator*]. FDP_IFF.1.3

5.2.3.3.6.4 The TSF shall provide the following: [{*additional capabilities chosen by the Security Target author*}]. FDP_IFF.1.4

5.2.3.3.6.5 The TSF shall explicitly authorize an information flow based on the following rules: [none]. FDP_IFF.1.5

5.2.3.3.6.6 The TSF shall explicitly deny an information flow based on the following rules: [{*additional rules chosen by the Security Target author*}]. FDP_IFF.1.6

5.2.3.3.7 Subset Residual Information Protection (FDP_RIP.1)

5.2.3.3.7.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] the following objects: [objects used to administer TOE security {*and other objects chosen by the Security Target author*}]. FDP_RIP.1.1

5.2.3.3.8 Basic Rollback (FDP_ROL.1)

5.2.3.3.8.1 The TSF shall enforce [mandatory access control policy] to permit the rollback of the [TOE System Administrator and TOE Security Administrator operations] on the [{*list of objects chosen by the Security Target author*}]. FDP_ROL.1.1

Application note: base the choice of objects on their ability to support rollback of all TOE administration operations.

5.2.3.3.8.2 The TSF shall permit operations to be rolled back within the [{*boundary limit to be chosen by the Security Target author*}]. FDP_ROL.1.2

5.2.3.4 Identification and Authentication (FIA)

5.2.3.4.1 Authentication Failure Handling (FIA_AFL.1)

5.2.3.4.1.1 The TSF shall detect when [a single-digit number, which can be preset by a TOE Security Administrator, of] unsuccessful authentication attempts occur related to [reauthentication or login]. FIA_AFL.1.1

Application note: during account creation, the TSF should configure the account to implement the preset number by default.

5.2.3.4.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [perform actions pre-specified by the TOE Security Administrator {*or other actions chosen by the Security Target author*} and alert all TOE Security Administrators and TOE System Administrators, providing the account identification and reason the TSF took action against the account]. FIA_AFL.1.2

Application note: an example of a pre-specified action would be for the TSF to lock the account from access after a specified number of unsuccessful authentication attempts.

5.2.3.4.2 User Attribute Definition (FIA_ATD.1)

5.2.3.4.2.1 The TSF shall maintain the following list of security attributes belonging to individual users: [identification data, role (user, TOE Security Administrator, TOE System Administrator), Community of Interest membership, nationality, authorization to export information out of the multinational information domain, authorization to receive information imported into the multinational information domain, {*and other user security attributes chosen by the Security Target author*}]. FIA_ATD.1.1

5.2.3.4.3 Timing of Authentication (FIA_UAU.2)

5.2.3.4.3.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. FIA_UAU.2.1

5.2.3.4.4 Multiple Authentication Mechanisms (FIA_UAU.5)

5.2.3.4.4.1 The TSF shall provide [password-based and token-based mechanisms] to support user authentication. FIA_UAU.5.1

Application note: the intent is to require multiple authentication mechanisms for remote administration of the TOE.

5.2.3.4.4.2 The TSF shall authenticate any user's claimed identity according to the [rule that remote administrators must be authenticated by password and token-based mechanisms]. FIA_UAU.5.2

5.2.3.4.5 Re-authenticating (FIA_UAU.6)

5.2.3.4.5.1 The TSF shall re-authenticate the user under the conditions: [FIA_UAU.6.1]

c) [Of user or administrator inactivity for a period of time that can be pre-set by a TOE Security Administrator,
d) When a TOE System Administrator creates a user account,
e) When a TOE Security Administrator changes the attributes associated with a user account, and
f) {*other conditions chosen by the Security Target author*}].

5.2.3.4.6 User Identification Before Any Action (FIA_UID.2)

5.2.3.4.6.1 The TSF shall require each user entity to identify itself before allowing any other TSF-mediated actions on behalf of that user. [FIA_UID.2.1]

5.2.3.4.7 User-Subject Binding (FIA_USB.1)

5.2.3.4.7.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user. [FIA_USB.1.1]

5.2.3.5 Security Management (FMT)

5.2.3.5.1 Management of Security Functions Behavior (FMT_MOF.1)

5.2.3.5.1.1 The TSF shall restrict the ability to [<u>determine the behavior of, disable, enable, and modify the behavior of</u>] the functions [of audit, authentication failure thresholds, profile-based anomaly thresholds, user attribute assignment, {*and functions chosen by the Security Target author*}] to [TOE Security Administrators]. [FMT_MOF.1.1]

Application note: the TOE shall provide user-friendly tools for TOE Security Administrators to perform these functions.

5.2.3.5.2 Management of Security Attributes (FMT_MSA.1) (Iteration 1)

5.2.3.5.2.1 The TSF shall enforce the [mandatory access control policy] to restrict the ability to [<u>change default, query, modify, or delete</u>] the security attributes [TOE Security Administrator, TOE System Administrator, author, releaser, recipient, {*and other attributes chosen by the Security Target author*}] to [TOE Security Administrators]. [FMT_MSA.1.1(1)]

5.2.3.5.3 Management of Security Attributes (FMT_MSA.1) (Iteration 2)

5.2.3.5.3.1 The TSF shall enforce the [mandatory access control policy] to restrict the ability to [<u>modify</u>] the security attributes [object sensitivity label {*and other attributes chosen by the Security Target author*}] to [the author of the object and TOE Security Administrators]. [FMT_MSA.1.1(2)]

5.2.3.5.4 Secure Security Attributes (FMT_MSA.2)

5.2.3.5.4.1 The TSF shall ensure that only secure values are accepted for security attributes. FMT_MSA.2.1

5.2.3.5.5 Static Attribute Initialization (FMT_MSA.3)

5.2.3.5.5.1 The TSF shall enforce the [mandatory access control policy] to provide [restrictive] default values for security attributes that are used to enforce the SFP. FMT_MSA.3.1

5.2.3.5.5.2 The TSF shall allow the [TOE Security Administrators] to specify alternative initial values to override the default values when an object or information is created. FMT_MSA.3.2

5.2.3.5.6 Management of TSF Data (FMT_MTD.1)

5.2.3.5.6.1 The TSF shall restrict the ability to [query] the [audit data {*and other data chosen by the Security Target author*}] to [TOE Security and System Administrators]. FMT_MTD.1.1

Application note: the TOE shall prevent any user or administrator from modifying the audit data. The audit data will not be deleted until it has been properly reviewed and archived in the TOE security environment.

5.2.3.5.7 Management of Limits on TSF Data (FMT_MTD.2)

5.2.3.5.7.1 The TSF shall restrict the specification of the limits for [age of backup data, size of audit files, and {*other data attributes as chosen by the Security Target author*}] to [TOE System Administrators]. FMT_MTD.2.1

5.2.3.5.7.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [alert all TOE Administrators and {*other actions to be specified by the Security Target author*}]. FMT_MTD.2.2

5.2.3.5.8 Secure TSF Data (FMT_MTD.3)

5.2.3.5.8.1 The TSF shall ensure that only secure values are accepted for TSF data. FMT_MTD.3.1

5.2.3.5.9 Revocation (FMT_REV.1)

5.2.3.5.9.1 The TSF shall restrict the ability to revoke security attributes associated with the [users, subjects, objects, **and cross-domain filtering functions**] within the TSC to [TOE Security Administrators]. FMT_REV.1.1

5.2.3.5.9.2 The TSF shall enforce the rules [prior to the next operation associated with the user, subject, object, or resource]. FMT_REV.1.2

5.2.3.5.10 Restrictions on Security Roles (FMT_SMR.2)

5.2.3.5.10.1 The TSF shall maintain the roles [user, TOE System Administrator, and TOE Security Administrator]. FMT_SMR.2.1

5.2.3.5.10.2 The TSF shall be able to associate users with roles. FMT_SMR.2.2

5.2.3.5.10.3 The TSF shall ensure that the conditions

c) [Non-administrative user accounts will not have administrator functions,
d) TOE System Administrator accounts will not have TOE Security Administrator functions, and
e) TOE Security Administrator accounts will not have TOE System Administrator functions]

are satisfied. FMT_SMR.2.3

5.2.3.5.11 Assuming Roles (FMT_SMR.3)

5.2.3.5.11.1 The TSF shall require an explicit request to assume the following roles: [TOE System Administrator and TOE Security Administrator]. FMT_SMR.3.1

5.2.3.6 Privacy (FPR)

5.2.3.6.1 Authorized User Observability (FPR_UNO.4)

5.2.3.6.1.1 The TSF shall provide [TOE Security Administrators] with the capability to observe the usage of [cross-domain transfer services and Community of Interest confidentiality services]. FPR_UNO.4.1

5.2.3.7 Protection of TOE Security Functions (FPT)

5.2.3.7.1 Abstract Machine Testing (FPT_AMT.1)

5.2.3.7.1.1 The TSF shall run a suite of tests [at the request of an authorized **TOE System Administrator or TOE Security Administrator**] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.[31] FPT_AMT.1.1

[31] Text was deleted from FPT_AMT.1.1. Rationale: the phrase "user" was replaced with "TOE system administrator or TOE security administrator" to properly define the requirement.

The TSF shall run a suite of tests [at the request of an authorized ~~user~~ TOE system administrator or TOE security administrator] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.2.3.7.2 Failure with Preservation of Secure State (FPT_FLS.1)

5.2.3.7.2.1 The TSF shall preserve a secure state when the following types of failures occur: [power failure, detection of an unauthorized or invalid operation, and {*other failures chosen by the Security Target author*}]. FPT_FLS.1.1

5.2.3.7.3 Inter-TSF Detection of Modification (FPT_ITI.1)

5.2.3.7.3.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [integrity protection equivalent to or better than SHA-1 and DSA or RSA]. FPT_ITI.1.1

5.2.3.7.3.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [an audit of the modification, notify the TOE Security Administrators, and retransmit the data] if modifications are detected. FPT_ITI.1.2

Application note: this requirement is intended to apply to audit data that is exported out of the TOE for storage and analysis.

5.2.3.7.4 Basic Internal TSF Data Transfer Protection (FPT_ITT.1)

5.2.3.7.4.1 The TSF shall protect TSF data from [modification] when it is transmitted between separate parts of the TOE. FPT_ITT.1.1

5.2.3.7.5 TSF Data Integrity Monitoring (FPT_ITT.3)

5.2.3.7.5.1 The TSF shall be able to detect [modification of data, substitution of data, re-ordering of data, and deletion of data] for TSF data transmitted between separate parts of the TOE. FPT_ITT.3.1

5.2.3.7.5.2 Upon detection of a data integrity error, the TSF shall take the following actions: [perform an audit of the modification, notify the TOE Security Administrators, and retransmit the data]. FPT_ITT.3.2

5.2.3.7.6 Notification of Physical Attack (FPT_PHP.2)

5.2.3.7.6.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF. FPT_PHP.2.1

5.2.3.7.6.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred. FPT_PHP.2.2

5.2.3.7.6.3 For [transmission security devices, cross-domain transfer systems, {*and devices or systems chosen by the Security Target author*}], the TSF shall monitor the devices and elements and notify [all TOE Security and System Administrators] when physical tampering with the TSF's devices or TSF's elements has occurred. FPT_PHP.2.3

5.2.3.7.7 Automated Recovery (FPT_RCV.2)

5.2.3.7.7.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided. FPT_RCV.2.1

5.2.3.7.7.2 For [electrical power interruption, network communication interruption, and {*other discontinuities chosen by the Security Target author*}], the TSF shall ensure the return of the TOE to a secure state using automated procedures. FPT_RCV.2.2

5.2.3.7.8 Domain Separation (FPT_SEP.1)

5.2.3.7.8.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. FPT_SEP.1.1

Application note: the intent of this requirement is to separate the security functionality from the operational functionality within the multinational environment that contains the TOE.

5.2.3.7.8.2 The TSF shall enforce separation between the security domains of subjects in the TSC. FPT_SEP.1.2

5.2.3.7.9 Reliable Time Stamps (FPT_STM.1)

5.2.3.7.9.1 The TSF shall be able to provide reliable time stamps for its own use. FPT_STM.1.1

5.2.3.7.10 TSF Testing (FPT_TST.1)

5.2.3.7.10.1 The TSF shall run a suite of self-tests [during initial start-up, periodically during normal operation, at the request of **an authorized TOE System Administrator or TOE Security Administrator**, during automatic recovery, {*and under other conditions chosen by the Security Target author*}] to demonstrate the correct operation of the TSF.[32] FPT_TST.1.1

5.2.3.7.10.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data. FPT_TST.1.2

5.2.3.7.10.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code. FPT_TST.1.3

[32] Text was deleted from FPT_TST.1.1. Rationale: replace the phrase "the authorized user" with "a system administrator or security administrator" to specify that the authorized users are administrators.

> The TSF shall run a suite of self-tests [during initial startup, periodically during normal operation, at the request of ~~the authorized user~~ a system administrator or security administrator, during automatic recovery, {*and other conditions chosen by the Security Target author*}] to demonstrate the correct operation of the TSF. FPT_TST.1.1

5.2.3.8 Resource Utilization (FRU)

5.2.3.8.1 Degraded Fault Tolerance (FRU_FLT.1)

5.2.3.8.1.1 The TSF shall [save all files being processed, if possible and fail safe] when the following failures occur: [loss of power, loss of network connection, hardware failure, or software failure].[33] FRU_FLT.1.1

Application note: if secure degraded operation is possible, such as during the loss of a network connection, then the TOE is not required to enter a fail safe mode.

5.2.3.9 TOE Access (FTA)

5.2.3.9.1 Per User Attribute Limitation on Multiple Concurrent Sessions (FTA_MCS.2)

5.2.3.9.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules: FTA_MCS.2.1

a) [A user logged in as a TOE Security Administrator cannot simultaneously initiate a session as a TOE System Administrator and
b) A user logged in as a TOE System Administrator cannot simultaneously initiate a session as a TOE Security Administrator].

5.2.3.9.1.2 The TSF shall enforce, by default, a limit of [a single-digit number, which can be preset by a TOE System Administrator, of] sessions per user. FTA_MCS.2.2

5.2.3.9.2 TSF-Initiated Session Locking (FTA_SSL.1)

5.2.3.9.2.1 The TSF shall lock an interactive session after [a time interval, which can be set by the user, up to a maximum limit configured by an authorized TOE Security Administrator] by: FTA_SSL.1.1

c) Clearing or overwriting display devices, making the current contents unreadable;
d) Disabling any activity of the user's data access/display devices other than unlocking the session.

Application note: the TSF will provide the ability for the TOE Security Administrator to set a default value that is implemented during the creation of each user account. The default value is not required to be equal to the maximum limit and should be less.

[33] Text was deleted from FRU_FLT.1.1. Rationale: the phrase "ensure the operation of" was deleted for better textual flow of the requirement.

The TSF shall ~~ensure the operation of~~ [save all files being processed, if possible and fail safe] when the following failures occur: [loss of power or network connection, hardware failure, or software failure]. FRU_FLT.1.1

5.2.3.9.2.2 The TSF shall require the following events to occur prior to unlocking the session: [user reauthentication, TOE Security Administrator authentication, {*or another event chosen by the Security Target author*}]. FTA_SSL.1.2

Application note: the TSF will provide the ability for a user or administrator to terminate the session, deactivate the system, or reboot the system if the session cannot be unlocked. Additionally, TOE Security Administrators may enter their authentication credentials (e.g., password) to unlock and resume a user session.

5.2.3.9.3 User-initiated Locking (FTA_SSL.2)

5.2.3.9.3.1 The TSF shall allow user-initiated locking of the user's own interactive session, by: FTA_SSL.2.1

c) Clearing or overwriting display devices, making the current contents unreadable;
d) Disabling any activity of the user's data access/display devices other than unlocking the session.

5.2.3.9.3.2 The TSF shall require the following events to occur prior to unlocking the session: [user reauthentication, TOE Security Administrator authentication, {*or another event chosen by the Security Target author*}]. FTA_SSL.2.2

Application note: the TSF will provide the ability for a user or administrator to terminate the session, deactivate the system, or reboot the system if the session cannot be unlocked. Additionally, TOE Security Administrators may enter their authentication credentials (e.g., password) to unlock and resume a user session.

5.2.3.9.4 Default TOE Access Banners (FTA_TAB.1)

5.2.3.9.4.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE. FTA_TAB.1.1

Application note: the content of the warning message shall be configurable by authorized TOE Security Administrators.

5.2.3.10 Trusted Path/Channels (FTP)

5.2.3.10.1 Inter-TSF Trusted Channel (FTP_ITC.1)

5.2.3.10.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. FTP_ITC.1.1

5.2.3.10.1.2 The TSF shall permit [the TSF] to initiate communication via the trusted channel. FTP_ITC.1.2

5.2.3.10.1.3 The TSF shall initiate communication via the trusted channel for [transferring audit data and {*for other functions to be determined by the Security Target author*}]. FTP_ITC.1.3

5.2.4 Transmission Security

For the transmission security category, this PP does not explicitly list security functional requirements. Instead, it incorporates by reference existing sources of transmission security functional requirements. Section 5.2.4.1 lists the references for inter-domain transmission security and Section 5.2.4.2 lists the references for intra-domain (such as the COIs in the MNIS Information Domain) transmission security.

5.2.4.1 Inter-Domain[34] Transmission Security

Two options exist for high assurance network encryption. Either option will meet the transmission security requirements for the MNIS TSE. The first option is to use virtual private network (VPN) solutions that have been evaluated by NSA and authorized for use with classified information. The second option is to use NSA approved (Type 1) encryption devices. The following two subsections provide references for each option.

5.2.4.1.1 Virtual Private Network Option

The DoD has published a basic robustness VPN PP (referenced below). However, a VPN protection profile for high robustness requirements, which is needed for the MNIS Environment, has not been published (a medium robustness VPN PP is in draft). Eventually, NSA may develop a VPN PP for high robustness use. Until it is available, use the functional requirements listed in the VPN PP for basic robustness and increase the assurance requirements from EAL level three to EAL level five. One additional requirement is that the VPN must be releasable for foreign military use.

The specific reference (available online at the Information Assurance Technical Forum web site[35]) is:

> *U.S. Department of Defense Virtual Private Network (VPN) Boundary Gateway Protection Profile For Basic Robustness Environments*, Release 0.6, 10 September 2001

5.2.4.1.2 High Assurance Encryption Device Option

The National Security Agency specifies high assurance encryption devices for the U.S. Government. Also, NSA helps determine whether encryption devices can be released for foreign military use, which is necessary in the MNIS situation.

---

[34] Section 2.3.2 discusses two uses of transmission security within the TSE. Each has its own set of security requirements. "Inter-Domain Transmission Security" refers to confidentiality and integrity requirements as protected information moves from one physical environment to another or between information domains.

[35] http://www.iatf.net/

For specific information regarding suitable encryption devices to use in a multinational information sharing situation, contact:

National Security Agency
Attn: IAD Business Affairs Office, V14
9800 Savage Road, Suite 6740
Fort George G. Meade, MD 20755-6740
Telephone: 410-854-7661

5.2.4.2 Intra-Domain[36] Transmission Security

As discussed in Section 2.2.2, a premise of the MNIS TOE is that medium robustness access controls and transmission security can be used within the MNIS Information Domain. The following two subsections provide references to existing protection profiles for less robust intra-domain transmission security options. The first discusses using VPN devices and the second subsection discusses another option.

5.2.4.2.1 Virtual Private Network Option

A properly configured VPN device satisfies the requirements for this COI privacy function. The basic VPN PP reference noted in 5.2.4.1.1 and repeated below documents the requirements:

> *U.S. Department of Defense Virtual Private Network (VPN) Boundary Gateway Protection Profile For Basic Robustness Environments*, Release 0.6, 10 September 2001

All requirements listed in the above reference are valid for intra-domain transmission security with the following exceptions:

1. Increase the assurance requirements from EAL level three to EAL level four;
2. Replace all references to "basic assurance" with "medium assurance and releasable for foreign military use"; and
3. Replace all references to "basic robustness" with "medium robustness and releasable for foreign military use."

5.2.4.2.2 Another Intra-Domain Privacy Option

There are other methods (rather than using VPNs and encryption devices) to implement medium robustness COI transmission security requirements. For example, a protection profile for multilevel operating systems in medium robustness environments exists. This PP appears to contain sufficient requirements to meet the needs of intra-domain transmission security. The specific reference (available online at the Information Assurance Technical Forum web site[37]) is:

---

[36] Section 2.3.2 discusses two uses of transmission security within the TSE. Each has its own set of security requirements. "Intra-Domain Transmission Security" refers to confidentiality and integrity requirements as protected information moves within the MNIS Domain while implementing COI needs.

[37] http://www.iatf.net/

Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness, Version 1.22, 23 May 2001

Another possible method for protecting the transmission of COI information is through the use of role based access controls (RBAC). However, an RBAC protection profile does not presently exist.

5.3 TOE Security Assurance Requirements

This section details security assurance requirements for the MNIS TOE for three of the four security categories that this PP identified in Section 2.3 (Access Control, Cross-Domain Filtering, and Security Administration). The assurance requirements for the fourth category (Transmission Security) are contained in the references provided in Section 5.2.4. Unless indicated in an application note, each assurance component applies to all three of the functional security categories (excluding Transmission Security). If a component does not apply to all three categories, an application note identifies which category is associated with the assurance component and also specifies the assurance component associated with the remaining categories.

The Evaluated Assurance Level (EAL) is EAL 5 Augmented for the Cross-Domain Filtering security category and is EAL 4 Augmented for the Access control and Security Administration categories. The rationale for the selection of these evaluated assurance levels is provided in Section 6.4.1.

5.3.1 Configuration Management (ACM)

ACM_AUT.2 Complete CM automation

ACM_AUT.2.1D The developer shall use a CM system.
ACM_AUT.2.2D The developer shall provide a CM plan.

ACM_AUT.2.1C The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation, and to all other configuration items.
ACM_AUT.2.2C The CM system shall provide an automated means to support the generation of the TOE.
ACM_AUT.2.3C The CM plan shall describe the automated tools used in the CM system.
ACM_AUT.2.4C The CM plan shall describe how the automated tools are used in the CM system.
ACM_AUT.2.5C The CM system shall provide an automated means to ascertain the changes between the TOE and its preceding version.
ACM_AUT.2.6C The CM system shall provide an automated means to identify all other configuration items that are affected by the modification of a given configuration item.

ACM_AUT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application note: ACM_AUT.2 (an EAL 6 component) is required only for the Cross-Domain Filtering category. ACM_AUT.1 (EAL 4) is sufficient for the Access Control and Security Administration categories.

ACM_CAP.4 Generation Support and Acceptance Procedures

ACM_CAP.4.1D The developer shall provide a reference for the TOE.
ACM_CAP.4.2D The developer shall use a CM system.
ACM_CAP.4.3D The developer shall provide CM documentation.

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.4.2C The TOE shall be labeled with its reference.
ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.
ACM_CAP.4.4C The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.4.5C The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.4.6C The CM system shall uniquely identify all configuration items.
ACM_CAP.4.7C The CM plan shall describe how the CM system is used.
ACM_CAP.4.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.4.10C The CM system shall provide measures such that only authorized changes are made to the configuration items.
ACM_CAP.4.11C The CM system shall support the generation of the TOE.
ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_SCP.3 Development tools CM coverage

ACM_SCP.3.1D The developer shall provide CM documentation.

ACM_SCP.3.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, security flaws, and development tools and related information.
ACM_SCP.3.2C The CM documentation shall describe how configuration items are tracked by the CM system.

ACM_SCP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application note: ACM_SCP.3 (an EAL 5 component) is required only for the Cross-Domain Filtering category. ACM_SCP.2 (EAL 4) is sufficient for the Access Control and Security Administration categories.

5.3.2 Delivery and Operation (ADO)

ADO_DEL.2 Detection of modification

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.2.2D The developer shall use the delivery procedures.

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.
ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

ADO_DEL.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, generation, and start-up procedures

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

ADV_FSP.3 Semiformal functional specification

ADV_FSP.3.1D The developer shall provide a functional specification.

ADV_FSP.3.1C The functional specification shall describe the TSF and its external interfaces using a semiformal style, supported by informal, explanatory text where appropriate.
ADV_FSP.3.2C The functional specification shall be internally consistent.
ADV_FSP.3.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.
ADV_FSP.3.4C The functional specification shall completely represent the TSF.
ADV_FSP.3.5C The functional specification shall include rationale that the TSF is completely represented.

ADV_FSP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.3.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

Application note: ADV_FSP.3 (an EAL 5 component) is required for the Cross-Domain Filtering category. ADV_FSP.2 (EAL 4) is sufficient for both the Access Control and Security Administration categories.

ADV_HLD.3 Semiformal high-level design

ADV_HLD.3.1D The developer shall provide the high-level design of the TSF.

ADV_HLD.3.1C The presentation of the high-level design shall be semiformal.
ADV_HLD.3.2C The high-level design shall be internally consistent.
ADV_HLD.3.3C The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.3.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.3.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.3.6C The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.3.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
ADV_HLD.3.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing complete details of all effects, exceptions and error messages.
ADV_HLD.3.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

ADV_HLD.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.3.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

Application note: ADV_HLD.3 (an EAL 5 component) is required for the three security categories.

ADV_IMP.2 Implementation of the TSF

ADV_IMP.2.1D The developer shall provide the implementation representation for the entire TSF.

ADV_IMP.2.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.
ADV_IMP.2.2C The implementation representation shall be internally consistent.
ADV_IMP.2.3C The implementation representation shall describe the relationships between all portions of the implementation.

ADV_IMP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_IMP.2.2E The evaluator shall determine that the implementation representation is an accurate and complete instantiation of the TOE security functional requirements.

Application note: ADV_IMP.2 (an EAL 5 component) is required for the three security categories.

ADV_INT.1 Modularity

ADV_INT.1.1D The developer shall design and structure the TSF in a modular fashion that avoids unnecessary interactions between the modules of the design.
ADV_INT.1.2D The developer shall provide an architectural description.

ADV_INT.1.1C The architectural description shall identify the modules of the TSF.
ADV_INT.1.2C The architectural description shall describe the purpose, interface, parameters, and effects of each module of the TSF.
ADV_INT.1.3C The architectural description shall describe how the TSF design provides for largely independent modules that avoid unnecessary interactions.

ADV_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_INT.1.2E The evaluator shall determine that both the low-level design and the implementation representation are in compliance with the architectural description.

Application note: ADV_INT.1 (an EAL 5 component) is required for the three security categories.

ADV_LLD.2 Semiformal low-level design

ADV_LLD.2.1D The developer shall provide the low-level design of the TSF.

ADV_LLD.2.1C The presentation of the low-level design shall be semiformal.
ADV_LLD.2.2C The low-level design shall be internally consistent.
ADV_LLD.2.3C The low-level design shall describe the TSF in terms of modules.
ADV_LLD.2.4C The low-level design shall describe the purpose of each module.
ADV_LLD.2.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.
ADV_LLD.2.6C The low-level design shall describe how each TSP-enforcing function is provided.
ADV_LLD.2.7C The low-level design shall identify all interfaces to the modules of the TSF.
ADV_LLD.2.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.
ADV_LLD.2.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing complete details of all effects, exceptions and error messages.
ADV_LLD.2.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

ADV_LLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_LLD.2.2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

Application note: ADV_LLD.2 (an EAL 6 component) is required for the three security categories.

ADV_RCR.2 Semiformal correspondence demonstration

ADV_RCR.2.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.2.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.
ADV_RCR.2.2C For each adjacent pair of provided TSF representations, where portions of both representations are at least semiformally specified, the demonstration of correspondence between those portions of the representations shall be semiformal.

ADV_RCR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application note: ADV_RCR.2 (an EAL 5 component) is required for the three security categories.

ADV_SPM.3 Formal TOE security policy model

ADV_SPM.3.1D The developer shall provide a TSP model.

ADV_SPM.3.2D The developer shall demonstrate, or prove, as appropriate, correspondence between the functional specification and the TSP model.

ADV_SPM.3.1C The TSP model shall be formal.
ADV_SPM.3.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.
ADV_SPM.3.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.
ADV_SPM.3.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.
ADV_SPM.3.5C Where the functional specification is semiformal, the demonstration of correspondence between the TSP model and the functional specification shall be semiformal.
ADV_SPM.3.6C Where the functional specification is formal, the proof of correspondence between the TSP model and the functional specification shall be formal.

ADV_SPM.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application note: ADV_SPM.3 (an EAL 5 component) is required for the Cross-Domain Filtering category. ADV_SPM.2 (EAL 4+) is sufficient for both the Access Control and Security Administration categories.

5.3.4 Guidance documents (AGD)

AGD_ADM.1 Administrator guidance

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.
AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_USR.1 User guidance

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.
AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Life Cycle Support (ALC)

ALC_DVS.1 Identification of security measures

ALC_DVS.1.1D The developer shall produce development security documentation.

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

ALC_FLR.3 Systematic flaw remediation

ALC_FLR.3.1D The developer shall provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.3.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.
ALC_FLR.3.3D The developer shall provide flaw remediation guidance addressed to TOE users.

ALC_FLR.3.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.3.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.3.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.3.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR.3.5C The flaw remediation procedures documentation shall describe a means by which the developer receives from TOE users reports and inquiries of suspected security flaws in the TOE.
ALC_FLR.3.6C The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.
ALC_FLR.3.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
ALC_FLR.3.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.
ALC_FLR.3.9C The flaw remediation procedures shall include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.
ALC_FLR.3.10C The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections.
ALC_FLR.3.11C The flaw remediation guidance shall identify the specific points of contact for all reports and inquiries about security issues involving the TOE.

ALC_FLR.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_LCD.2 Standardized life-cycle model

ALC_LCD.2.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.
ALC_LCD.2.2D The developer shall provide life-cycle definition documentation.

ALC_LCD.2.3D The developer shall use a standardized life-cycle model to develop and maintain the TOE.

ALC_LCD.2.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.
ALC_LCD.2.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.
ALC_LCD.2.3C The life-cycle definition documentation shall explain why the model was chosen.
ALC_LCD.2.4C The life-cycle definition documentation shall explain how the model is used to develop and maintain the TOE.
ALC_LCD.2.5C The life-cycle definition documentation shall demonstrate compliance with the standardized life-cycle model.

ALC_LCD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application note: ALC_LCD.2 (an EAL 5 component) is required by the Cross-Domain Filtering category. ALC_LCD.1 (EAL 4) is sufficient for both the Access Control and Security Administration categories.

ALC_TAT.2 Compliance with implementation standards--all parts

ALC_TAT.2.1D The developer shall identify the development tools being used for the TOE.
ALC_TAT.2.2D The developer shall document the selected implementation-dependent options of the development tools.
ALC_TAT.2.3D The developer shall describe the implementation standards to be applied.

ALC_TAT.2.1C All development tools used for implementation shall be well-defined.
ALC_TAT.2.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.
ALC_TAT.2.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

ALC_TAT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_TAT.2.2E The evaluator shall confirm that the implementation standards have been applied.

Application note: ALC_TAT.2 (an EAL 5 component) is required by the Cross-Domain Filtering category. ALC_TAT.1 (EAL 4) is sufficient for both the Access Control and Security Administration categories.

5.3.6 Tests (ATE)

ATE_COV.3 Rigorous Analysis of Coverage

ATE_COV.3.1D The developer shall provide an analysis of the test coverage.

ATE_COV.3.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.3.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.
ATE_COV.3.3C The analysis of the test coverage shall rigorously demonstrate that all external interfaces of the TSF identified in the functional specification have been completely tested.

ATE_COV.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application note: ATE_COV.3 (an EAL 6 component) is required by both the Cross-Domain Filtering and System Administration categories. ATE_COV.2 (EAL 4) is sufficient for the Access Control Category.

ATE_DPT.2 Testing: low-level design

ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.2.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design and low-level design.

ATE_DPT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application note: ATE_DPT.2 (an EAL 5 component) is required for the three security categories.

ATE_FUN.2 Ordered Functional Testing

ATE_FUN.2.1D The developer shall test the TSF and document the results.
ATE_FUN.2.2D The developer shall provide test documentation.

ATE_FUN.2.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.2.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.2.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.2.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.2.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.
ATE_FUN.2.6C The test documentation shall include an analysis of the test procedure ordering dependencies.

ATE_FUN.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application note: ATE_FUN.2 (an EAL 6 component) is required for the three security categories.

ATE_IND.2 Independent Testing -- Sample

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.
ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability Assessment (AVA)

Application note: Vulnerability Analysis will have to be performed in the System context. Vulnerability analysis results from components will likely still be valid in the System, but the System may very well introduce new potential vulnerabilities in integrating the components.

AVA_CCA.1 Covert channel analysis

AVA_CCA.1.1D The developer shall conduct a search for covert channels for each information flow control policy.
AVA_CCA.1.2D The developer shall provide covert channel analysis documentation.

AVA_CCA.1.1C The analysis documentation shall identify covert channels and estimate their capacity.
AVA_CCA.1.2C The analysis documentation shall describe the procedures used for determining the existence of covert channels, and the information needed to carry out the covert channel analysis.
AVA_CCA.1.3C The analysis documentation shall describe all assumptions made during the covert channel analysis.

AVA_CCA.1.4C The analysis documentation shall describe the method used for estimating channel capacity, based on worst case scenarios.
AVA_CCA.1.5C The analysis documentation shall describe the worst case exploitation scenario for each identified covert channel.

AVA_CCA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_CCA.1.2E The evaluator shall confirm that the results of the covert channel analysis show that the TOE meets its functional requirements.
AVA_CCA.1.3E The evaluator shall selectively validate the covert channel analysis through testing.

Application note: AVA_CCA.1 (an EAL 5 component) is required only for the Cross Domain Filtering category.

AVA_MSU.3 Analysis and Testing for Insecure States

AVA_MSU.3.1D The developer shall provide guidance documentation.
AVA_MSU.3.2D The developer shall document an analysis of the guidance documentation.

AVA_MSU.3.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.
AVA_MSU.3.2C The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.3.3C The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.3.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_MSU.3.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

AVA_MSU.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_MSU.3.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.
AVA_MSU.3.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.
AVA_MSU.3.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.
AVA_MSU.3.5E The evaluator shall perform independent testing to determine that an administrator or user, with an understanding of the guidance documentation, would reasonably be able to determine if the TOE is configured and operating in a manner that is insecure.

Application note: AVA_MSU.3 (an EAL 6 component) is required by the Cross-Domain Filtering category. AVA_MSA.2 (EAL 4) is sufficient for both the Access Control and Security Administration categories.

AVA_SOF.1 Strength of TOE security function evaluation

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

AVA_VLA.3 Moderately Resistant

AVA_VLA.3.1D The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.
AVA_VLA.3.2D The developer shall document the disposition of identified vulnerabilities.

AVA_VLA.3.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
AVA_VLA.3.2C The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.
AVA_VLA.3.3C The evidence shall show that the search for vulnerabilities is systematic.

AVA_VLA.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.3.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.
AVA_VLA.3.3E The evaluator shall perform an independent vulnerability analysis.
AVA_VLA.3.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.
AVA_VLA.3.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a moderate attack potential.

Application note: AVA_VLA.3 (an EAL 5 component) is required for the three security categories.

6 - Rationale

This chapter provides the rationale for the selection of the TOE security policies, the threats to TOE security, and the security objectives for the TOE. Section 6.1 provides the rationale for the existence of the security objectives based upon the stated threats and security policies. Section 6.2 provides the rationale for the MNIS TOE security objectives. Section 6.3 provides the rationale for the TOE security functional requirements and Section 6.4 provides the rationale for the TOE security assurance requirements. Section 6.5 includes a table of dependencies, showing that all dependencies have been met in this Protection Profile and Section 6.6 provides the robustness rationale for the MNIS TOE.

6.1 Threats and Policies Rationale

Each identified threat to security that is not completely addressed by one or more assumptions results in a security objective. Each identified security policy leads to one or more security objectives unless assumptions satisfy the policy. As described in Section 4.1, each objective reflects the stated intent of the TOE to counter the threats identified and adhere to applicable policies while taking into consideration the relevant assumptions. The resulting security objectives[38] may be associated with more than one threat to the TOE security or security policy statement.

Table 5 summarizes the relationship between the threats to TOE security and the TOE security objectives. The table also summarizes the relationship between the security policies associated with the MNIS Environment to the TOE security objectives. It demonstrates coverage of each threat and security policy.

Table 5 - Mapping of Threats and Policies to Security Objectives

	O.AUDIT	O.AUTHENTICATION	O.AUTHORIZED_USE	O.CROSS_DOMAIN_FILTERING	O.ERROR_REJECT	O.MANAGE	O.NON-REPUDIATION	O.PROHIBIT_MALICIOUS_CODE	O.PROTECT	O.PROTECT_EXT_COMMS	O.REACT	O.RECOVERY	O.TOE_FAILSAFE
T.ACCESS_ELECTRONIC	X	X	X	X	X					X	X		
T.ACCESS_PHYSICAL		X	X								X		
T.ALARM_FAIL	X				X	X		X			X		
T.AUDIT_FAIL	X				X	X		X			X		
T.AUTHORIZATION_EXCEED	X	X	X	X	X		X		X				

[38] The rationale incorporates all TOE objectives and some TOE Security Environment (TSE) objectives (OE). A TSE objective is included when deemed necessary.

	O.AUDIT	O.AUTHENTICATION	O.AUTHORIZED_USE	O.CROSS_DOMAIN_FILTERING	O.ERROR_REJECT	O.MANAGE	O.NON-REPUDIATION	O.PROHIBIT_MALICIOUS_CODE	O.PROTECT	O.PROTECT_EXT_COMMS	O.REACT	O.RECOVERY	O.TOE_FAILSAFE
T.COMPROMISE_CRYPTO										X	X	X	X
T.DENIAL_OF_SERVICE	X										X	X	
T.DISASTER_ENVIRO	X					X					X	X	X
T.ERROR_ADMIN	X					X			X		X	X	
T.ERROR_USER	X				X	X			X		X	X	
T.IMPERSONATE	X	X	X								X		
T.IMPORT_BAD	X			X	X			X			X	X	
T.MALICIOUS_ADMIN	X		X				X	X	X		X	X	
T.MALICIOUS_USER	X		X				X	X	X		X	X	
T.POOR_ADMIN	X				X	X			X		X	X	
T.POOR_BACKUP	X					X						X	
T.POOR_IMPLEMENTATION												X	X
T.POOR_TRAIN	X				X	X			X		X	X	
T.REPUDIATE	X	X	X				X						
T.TOE_FAIL	X				X						X	X	X
P.ACCOUNTABILITY	X	X	X				X		X				
P.ADMIN_SECURITY									X		X	X	
P.ADMIN_SPLIT	X	X	X		X	X	X		X		X		
P.ADMIN_SYSTEM	X					X			X		X		
P.AUDIT_REVIEW	X								X		X		
P.CROSS_DOMAIN_FILTERING	X	X	X	X				X	X				
P.DISTRIBUTION								X					
P.DUE_CARE	X	X	X	X	X	X	X	X	X	X	X	X	
P.MNIS_ENVIRON_EXTERNAL_DISTRO	X								X	X			
P.MNIS_ENVIRON_INTERNAL_DISTRO	X	X	X					X	X		X		
P.MNIS_INFO_PROTECT	X		X						X				
P.MNIS_INFO_RECIPIENTS	X	X		X			X		X				
P.MNIS_INFO_SENDERS	X	X	X	X			X		X				
P.MNIS_INFO_SOURCES	X	X		X			X		X				
P.REJECT_PARTNER_INFO	X			X				X	X		X		
P.REJECT_U.S._INFO	X			X				X			X		
P.SECURITY_ADMIN_RESTRICTED	X	X	X				X						
P.USERS	X	X	X				X		X				

6.1.1 Rationale for Threats

T.ACCESS_ELECTRONIC - *An unauthorized agent may gain network access to the TOE and thereby compromise its secure operation.*

Because the TOE is used by a multinational partnership, the TOE is a target for unauthorized access by adversaries (A.THREAT_LEVEL). Certain policies and assumptions will counter this threat (A.AUDIT_ANALYSIS, A.POLICY_MNIS, A.POLICY_US_REL-LAN, A.TOE_USER_AUTHENTICATION, and A.TRANSEC_CRYPTO). To detect attacks from outside adversaries, the TOE will scrutinize all network traffic entering the MNIS information domain (O.CROSS_DOMAIN_FILTERING) and will audit all activities (O.AUDIT, O.AUTHENTICATION, and O.AUTHORIZED_USE). The TOE shall block attempts to gain unauthorized access (O.ERROR_REJECT and O.PROTECT_EXT_COMMS) and notify TOE administrative personnel (O.REACT) of violations.

T.ACCESS_PHYSICAL - *An unauthorized agent may gain physical access to the TOE and thereby compromise its secure operation.*

The threat of unauthorized physical access (A.THREAT_LEVEL) to the TOE is greatly mitigated by certain assumptions (A.PHYSICAL_SECURITY, A.TOE_DESIGN, and A.TOE_USER_AUTHENTICATION). However, the TOE shall control access to its systems and components in case an unauthorized agent successfully gains physical access to the TOE (O.AUTHENTICATION and O.AUTHORIZED_USE) to stop the agent from using any TOE systems or applications. The TOE shall notify administrative personnel (O.REACT) of detected violations.

T.ALARM_FAIL - *Failure of intrusion detection systems, alerting systems, or alarms may allow unauthorized activity to occur without detection or security response.*

The threat of a failure in TOE detection and alarm systems (A.THREAT_LEVEL) is addressed by underlying assumptions (A.CONFIGURATION, A.TOE_MAINTENANCE, A.COMPLY, and A.TOE_OPERATION). Given that an alarm might fail, the TOE shall provide specific defenses to track all activity (O.AUDIT) and reject errors and malicious activity (O.ERROR_REJECT and O.PROHIBIT_MALICIOUS_CODE). The TOE shall inform administrative personnel of the situation (O.REACT) and provide useful administrative capabilities to respond to the situation (O.MANAGE).

T.AUDIT_FAIL - *System modification, compromise, or audit file "full" may result in an audit failure.*

Failure of the audit system or loss of audit data may is addressed by the assumptions A.TRAINED, A.TOE_MAINTENANCE, and A.TOE_OPERATION. However, attacks on the audit system compel the need to reject malicious errors (O.PROHIBIT_MALICIOUS_CODE and O.ERROR_REJECT). Inadvertent errors can be mitigated if administrative procedures and tools are easy to use (O.AUDIT). Immediate administrative response can reduce the likelihood that the audit file may become full (O.REACT).

T.AUTHORIZATION_EXCEED - *Authorized users may access data or resources for which they are not authorized.*

The TOE is designed to prohibit authorized users (A.TOE_USER) and processes from gaining access to data or resources beyond their authorization (A.TOE_USER_AUTHENTICATION, A.COI, A.CLEARANCE, A.INFORMATION_VALUE, and A.MNIS_INFO_INTERNAL). New personnel (A.DYNAMIC_PARTNERSHIP) are trained to properly use the TOE (A.TRAINED) so that unauthorized information does not enter the MNIS Information Domain (A.MNIS_INFO_CLASSIFICATION). Unauthorized access (O.AUTHENTICATION, O.AUTHORIZED_USE, and O.NON-REPUDIATION), whether accidental or malicious, must be tracked (A.AUDIT_ANALYSIS and O.AUDIT). The TOE shall protect against errors (O.PROTECT and O.ERROR_REJECT) that might compromise information. The TOE shall prohibit attempts to import or export unauthorized data across security domain boundaries (O.CROSS_DOMAIN_FILTERING).

T.COMPROMISE_CRYPTO - *Unauthorized agents may attack TOE cryptographic components using cryptanalysis or social engineering and compromise the secure operation of the TOE.*

The TOE implementation must comply with applicable cryptographic policies and regulations (A.COMPLY, A.CONFIGURATION, and A.THREAT_LEVEL) and it is assumed that cryptographic components are properly selected, installed, and operated (A.CONNECTIONS, A.TOE_OPERATION, and A.TRANSEC_CRYPTO) to support secure TOE operations (A.CRYPTO_SUPPORT). The cryptographic components shall provide confidentiality and integrity protection for the data (O.PROTECT_EXT_COMMS) and be able to prevent cryptographic attacks (O.REACT) and resume normal operations (O.RECOVERY). If necessary, the cryptographic mechanisms shall terminate external communications to protect the confidentiality and integrity of TOE data (O.TOE_FAILSAFE).

T.DENIAL_OF_SERVICE - *An unauthorized agent may intentionally compromise the availability of the TOE with a denial of service attack.*

Adversaries are assumed to be sophisticated (A.THREAT_LEVEL) and a residual insider threat remains (A.MNIS_INFO_ACCESSIBLE). Adequate communications capability exists to counter this threat (A.COMMS_AVAILABLE), but the TOE shall be able to identify (O.REACT) and recover (O.RECOVERY) from denial of service attacks. The audit system (O.AUDIT) will help to identify the source of the attacks.

T.DISASTER_ENVIRO - *Environmental disasters may compromise the secure operation of the TOE.*

The design, implementation, maintenance, and operation of the TOE will safeguard against some environmental disasters (A.BACK_UP, A.COMPLY, A.CONFIGURATION, A.LOGISTICS_SUPPORT, and A.TOE_DESIGN). Authorized administrators will be available to take action against other catastrophic events (A.ADMIN_AVAILABLE). Accordingly, the TOE shall provide user-friendly administration tools (O.MANAGE), it shall identify and react to catastrophic events (O.AUDIT and O.REACT), and it shall implement predefined procedures

that will help quickly restore secure TOE operation (O.RECOVERY). If necessary, the TOE shall be able to quickly stop affected systems in a secure configuration (O.TOE_FAILSAFE).

T.ERROR_ADMIN - *TOE administrator error may violate security policy, compromise information, or degrade secure TOE operation.*

Improper TOE administration could result if an administrator is incompetent, unknowledgeable, or less trustworthy than expected. Assumptions A.TRAINED, A.TOE_OPERATION, and A.PERSONNEL_TRUST address these possibilities. Furthermore, audit analysis (A.AUDIT_ANALYSIS) can help to identify administrator error, while back up mechanisms (A.BACK_UP) will help recover from administrator error. However, these features depend on an auditing capability (O.AUDIT) and administrator procedures and tools (O.MANAGE). If an administrator error occurs, the TOE shall automatically be able to protect itself (O.ERROR_REJECT, O.PROTECT, and O.REACT) and initiate recovery from the error (O.RECOVERY). Finally, split administrator duties (OE.SPLIT_ADMIN) reduce the likelihood of administrator error.

T.ERROR_USER - *An authorized user may perform erroneous actions that will violate security policy, compromise information, or corrupt information integrity.*

Untrained or incompetent users may perform unauthorized actions (A.TRAINED), although they are trusted to not perform malicious errors (A.PERSONNEL_TRUST). The changing nature of coalition membership (A.DYNAMIC_PARTNERSHIP) may increase the likelihood of user error. External analysis capabilities exist to identify user errors (A.AUDIT_ANALYSIS) and backup mechanisms exist to help mitigate these errors (A.BACK_UP). Therefore, individual actions shall be audited (O.AUDIT) to provide the ability for the TOE to automatically identify, reject, and respond to user errors (O.ERROR_REJECT, O.PROTECT, and O.REACT). The TOE shall include capabilities to help restore secure TOE operation (O.MANAGE and O.RECOVERY) to reduce the likelihood of information compromise.

T.IMPERSONATE - *An unauthorized agent may attempt to gain network access to the TOE or the information it protects by pretending to be an authorized user or administrator.*

U.S. and multinational policies will require users and processes to be authenticated prior to TOE access (A.TOE_USER_AUTHENTICATION, A.POLICY_MNIS, and A.POLICY_US_REL-LAN). The expected threat level (A.THREAT_LEVEL) indicates that impersonation might occur. It is assumed that all attempted and successful access attempts will be analyzed to ensure that they are authorized (A.AUDIT_ANALYSIS). The TOE shall audit access attempts (O.AUDIT) and react (O.REACT) to unauthorized use (O.AUTHENTICATION and O.AUTHORIZED_USE).

T.IMPORT_BAD - *Unauthorized code, to include malicious code, may be introduced into the TOE, resulting in a compromise to its secure operation.*

Due to the expected threat level (A.THREAT_LEVEL), the U.S. and multinational partners will develop policies that require the TOE to reject malicious code (A.POLICY_MNIS and

A.POLICY_US_REL-LAN). External audit analysis (A.AUDIT_ANALYSIS) and file backups will help mitigate the impact of malicious code. The TOE shall block attempts to introduce malicious code into the TOE (O.CROSS_DOMAIN_FILTERING, O.ERROR_REJECT, and O.PROHIBIT_MALICIOUS_CODE). The TOE will audit all data transfers into the TOE (O.AUDIT) for later review. When malicious code is detected, the TOE shall attempt to mitigate the attack (O.REACT) and return to secure operation (O.RECOVERY).

T.MALICIOUS_ADMIN - *Occasionally an administrator maliciously attempts to undermine the function of the TOE.*

The administrative functions are vital to secure TOE operation (A.TOE_OPERATION). All administrators shall be authorized and cleared for their duties (A.CLEARANCE), yet an administrator might be less trustworthy than expected (A.PERSONNEL_TRUST and A.THREAT_LEVEL). Mechanisms outside of the TOE will help to identify malicious administrator activity (A.AUDIT_ANALYSIS). Therefore, complete auditing of individual administrator activities (O.AUDIT, O.AUTHORIZED_USE, and O.NON-REPUDIATION) is necessary. Mechanisms within the TOE shall not allow administrator misconduct to compromise sensitive information (O.ERROR_REJECT, O.PROHIBIT_MALICIOUS_CODE, and O.PROTECT). The TOE must include countermeasures that can respond automatically to abuse and implement predefined activities to help restore secure TOE operation (O.REACT and O.RECOVERY).

T.MALICIOUS_USER - *Occasionally an authorized user maliciously attempts to undermine the function of the TOE.*

The TOE must restrict authorized users from maliciously misusing their privileges. A number of assumptions address this threat (A.AUDIT_ANALYSIS, A.CLEARANCE, A.MISSION, A.PERSONNEL_TRUST, A.TOE_OPERATION, and A.TOE_USER). However, the threat of malicious activity is high (A.COI, A.DYNAMIC_PARTNERSHIP, and A.THREAT_LEVEL). Therefore, the TOE shall protect itself against malicious user actions (O.ERROR_REJECT, O.AUTHORIZED_USE, O.PROHIBIT_MALICIOUS_CODE, O.PROTECT, O.REACT, and O.RECOVERY) and shall associate all malicious activity with the appropriate individual (O.NON-REPUDIATION and O.AUDIT).

T.POOR_ADMIN - *Poor systems and security administration may compromise the secure operation of the TOE. For example, administrators may fail to review configuration settings periodically, install system and security patches, or take appropriate actions in response to audit analysis alerts.*

Contrasted with T.ERROR_ADMIN, this threat results from administrator inaction or inattention, and not from an error. However, assumptions A.PERSONNEL_TRUST, A.TRAINED, A.TOE_MAINTENANCE, and A.TOE_OPERATION address this threat. Also, audit analysis (A.AUDIT_ANALYSIS) helps to identify when administration is poor; this depends on an audit capability (O.AUDIT). To improve administrator performance (OE.GOOD_ADMIN), the TOE shall be designed to provide user-friendly administration tools

(O.MANAGE) in support of due diligence (OE.DUE_CARE). If poor administration results in an error or non-secure situation, the TOE shall reject the error (O.ERROR_REJECT), protect against information compromise (O.PROTECT), and return to secure operation (O.REACT and O.RECOVERY).

T.POOR_BACKUP - *Failure to adequately perform system backup may result in compromise of TOE operation or loss of user data.*

All TOE data (A.INFORMATION_VALUE) is regularly backed up (A.BACK_UP). Administrative personnel are trained in proper TOE operation (A.TRAINED and A.TOE_OPERATION) so that backup procedures are not overlooked. However, people make mistakes, so the TOE shall be designed to provide user-friendly backup tools (O.MANAGE). Furthermore, the TOE shall audit (O.AUDIT) administrator actions, and, if necessary, the TOE shall provide the capability to recover (O.RECOVERY) from administrator error.

T.POOR_IMPLEMENTATION - *Due to poor design or improper implementation of the TOE it may not operate in a secure manner.*

Faults in the TOE's implementation can be reduced by proper design (A.COMPLY, A.CONFIGURATION, A.TEMPEST, and A.TOE_DESIGN) and operation (A.SPONSOR and A.TRAINED). However, if poor implementation results in a security failure, the TOE shall transition to a secure state (O.TOE_FAILSAFE) or at least be able to recover to a secure state (O.RECOVERY).

T.POOR_TRAIN - *Insufficient training may result in insecure operation of the TOE.*

By policy (A.POLICY_MNIS and A.POLICY_US_REL-LAN), TOE users are properly trained (A.TRAINED) and cleared (A.CLEARANCE). But training failures, incompetent personnel, or personnel changes (A.DYNAMIC_PARTNERSHIP) are expected to reduce the effectiveness of training. External analysis capabilities exist to identify user errors (A.AUDIT_ANALYSIS) and backup mechanisms exist to help mitigate these errors (A.BACK_UP). Therefore, individual actions shall be audited (O.AUDIT) to provide the ability for the TOE to automatically identify, reject, and respond to user errors (O.ERROR_REJECT, O.PROTECT, and O.REACT). The TOE shall include capabilities to help restore secure TOE operation (O.MANAGE and O.RECOVERY) to reduce the likelihood of information compromise.

T.REPUDIATE - *Authorized users or administrators may deny performing actions that they did perform.*

Authorized TOE personnel (A.TOE_USER) may try to hide or deny their use of the TOE. New users (A.DYNAMIC_PARTNERSHIP) may be confused about the outcome of their actions. Audit analysis (A.AUDIT_ANALYSIS) will help identify the actions of authorized users and administrators (A.TOE_USER_AUTHENTICATION). Therefore, the TOE shall audit all security-relevant activities (O.AUDIT) by each individual TOE user or administrator (O.AUTHENTICATION and O.AUTHORIZED_USE), identifying the specific individual (O.NON-REPUDIATION).

T.TOE_FAIL - *TOE component or software failure may cause the TOE to operate in an insecure manner.*

It is assumed that proper design, support, configuration control, and management will ensure that a TOE failure does not unacceptably degrade security (A.ADMIN_AVAILABLE, A.CONFIGURATION, A.LOGISTICS_SUPPORT, A.TOE_DESIGN, and A.TOE_MAINTENANCE). The security impact of TOE failures is further mitigated because all users are authorized access to Secret information (A.CLEARANCE), lost data can be recovered (A.BACK_UP), and audit analysis outside of the TOE will be able to identify the impact of the system failure (A.AUDIT_ANALYSIS and O.AUDIT). Failures are expected during the life of the TOE, so the TOE shall be able to degrade gracefully and recover from failures without compromising security (O.ERROR_REJECT, O.REACT, and O.RECOVERY) or, if recovery is not possible, the TOE shall shut down to a secure mode (O.TOE_FAILSAFE).

6.1.2 Rationale for Policies

P.ACCOUNTABILITY - *Authorized administrators and users are held accountable for security relevant actions they perform.*

In any well-managed IT system, users and administrators must be held responsible for actions they take that affect the secure operation of the TOE. This policy leads to the assumptions that at least one TOE Security Administrator is on duty at all time (A.ADMIN_AVAILABLE) and that audit analysis information is available to the administrator on a continuous basis (A.AUDIT_ANALYSIS). We also assume that it is important to authenticate each user and administrator before granting access to information assets (A.TOE_USER_AUTHENTICATION). Every user and administrator is cleared to a Secret level even though they may not have the need to know all the information (A.SYSTEM_HIGH) and personnel are trusted to do their jobs correctly (A.PERSONNEL_TRUST). Also important is that backups of security relevant parameters, system files, and user files are performed correctly and routinely (A.BACK_UP).

The policy on personnel accountability gives rise to several relevant TOE objectives. Accountability necessitates auditing (O.AUDIT), authentication (O.AUTHENTICATION), and non-repudiation (O.NON-REPUDIATION) within the TOE to permit only approved personnel use (O.AUTHORIZED_USE). Also, it leads to the objective that the TOE protects itself against intentional and unintentional compromises of information by authorized personnel (O.PROTECT).

The policy on personnel accountability also gives rise to five TOE environmental objectives. One fundamental principle is to split the duties of the critical administration job with all its inherent privileges (OE.SPLIT_ADMIN). Another is to route the audit files to a misuse detection system for detailed analysis of security relevant issues (OE.MISUSE_DETECTION). These objectives promote the fact that the management of the TOE must provide for “due care” of its valuable resources (OE.DUE_CARE).

P.ADMIN_SECURITY - *A Security Administrator interprets, maintains, and oversees site security policy and develops and implements procedures assuring secure operation of the TOE.*

In any well-managed IT environment, management has developed a security policy and assigned its implementation to the security administrator staff. Management frequently checks (A.AUDIT_ANALYSIS) to ensure that the security staff is faithfully carrying out their developed and published policy. This policy leads to the assumptions that a competent security staff is in place (A.ADMIN_AVAILABLE), that the staff has developed a management approved (A.SPONSOR and A.COMPLY) security policy for the TOE and its environment (A.BACK_UP, A.POLICY_MNIS, A.POLICY_US_REL-LAN), and that automated tools available for the staff to carry out the security policies effectively and efficiently (A.TOE_OPERATION). All policies assume that personnel are trusted (A.PERSONNEL_TRUST), trained (A.TRAINED), and authenticated before being given access to the TOE (A.TOE_USER_AUTHENTICATION).

This policy and related assumptions lead to several objectives. The policy is to protect (O.PROTECT) the TOE from failure. If a failure does occur, the TOE must react (O.REACT) and recover (O.RECOVERY). Two environmental objectives are noteworthy. OE.SPLIT_ADMIN and OE.SPLIT_ADMIN_SECURITY emphasize the importance of employing sufficient security personnel. TOE security administration cannot be an additional duty assigned to a busy system administrator.

P.ADMIN_SPLIT - *Administrative responsibilities are split between System Administrator and Security Administrator roles that together competently administer the TOE. The assignment of split administrative authorization is established in order to prevent unrestricted system control and to provide for "checks and balances."*

The multinational TOE (which is a military command and control environment) is too important (A.INFORMATION_VALUE) to allow one administrator to have total control. Assumptions regarding personnel availability (A.ADMIN_AVAILABLE and A.TOE_MAINTENANCE), their trust-worthiness (A.PERSONNEL_TRUST), the environment in which they work (A.SYSTEM_HIGH and A.THREAT_LEVEL), and the tools that they have available to effectively do their job (A.AUDIT_ANALYSIS), all affect this policy.

To effectively implement this policy, critical security events must be audited (O.AUDIT) and administrators must be authenticated prior to access of authorized TOE resources (O.AUTHENTICATION and O.AUTHORIZED_USE). Also, the system must be able to reject inadvertent administrator errors (O.ERROR_REJECT). This translates into systems that are user friendly (O.MANAGE). There must be strong non-repudiation mechanisms in the system so that administrators are held responsible for actions they take (O.NON-REPUDIATION). In general, the TOE must be able to protect (O.PROTECT) itself and react (O.REACT) to attacks on it.

There are several environmental objectives closely tied to this policy. A direct outcome of this policy is the need for split administrative responsibilities within the TOE environment (OE.SPLIT_ADMIN, OE.SPLIT_ADMIN_SECURITY and OE.SPLIT_ADMIN_SYSTEM). Also, misuse detection (OE.MISUSE_DETECTION) is important to monitor split administration.

P.ADMIN_SYSTEM - *A System Administrator is responsible for installing, configuring, managing, and monitoring the performance of the TOE in accordance with its evaluated configuration and ensuring its conformance to applicable security policies.*

The TOE System Administrators have super-user privileges because of their broad responsibilities (A.TOE_MAINTENANCE and A.TOE_OPERATION). Therefore, they must be trained (A.TRAINED) and competent (OE.GOOD_ADMIN) to ensure they do no harm. Additionally, administrators are trusted (A.PERSONNEL_TRUST) and authorized (A.TOE_USER_AUTHENTICATION) to perform their duties in compliance with policy (A.COMPLY). Administrators are available (A.ADMIN_AVAILABLE and A.SPONSOR), tools are available to do the job (A.AUDIT_ANALYSIS, A.BACK_UP, A.LOGISTICS_SUPPORT, and A.TOE_DESIGN), and the physical environment is relatively benign and well protected (A.PHYSICAL_SECURITY and A.CONNECTIONS).

The TOE must be designed to protect (O.PROTECT), detect (OE.MISUSE_DETECT), and respond (O.REACT) to attacks. Auditing (O.AUDIT) is an important component of detection and the sponsoring Command must provide and promote good management practices (O.MANAGE).

P.AUDIT_REVIEW - *Administrators and users will review audit reports and take appropriate action.*

Auditing is a vital tool to spot a variety of problems (including attacks) and audit analysis (OE.MISUSE_DETECTION) must be performed consistently (A.AUDIT_ANALYSIS). System backups are necessary for audit research and system recovery (A.BACK_UP). Personnel are trusted to comply with proper procedures and policy (A.COMPLY and A.PERSONNEL_TRUST). This requires proper selection of the security relevant events to be audited and accurate audit records (O.AUDIT). This enables administrators to react (O.REACT) to attacks and to protect (O.PROTECT) the TOE.

P.CROSS_DOMAIN_FILTERING - *Information domains will not be directly connected without application of appropriate cross-domain filtering techniques.*

This policy is one of the main tenets of Defense in Depth and personnel must comply with it (A.COMPLY). There must be protection at interconnections (O.PROTECT) between information domains (O.CROSS_DOMAIN_FILTERING) because of the different access controls, need-to-know, and levels of protection in each domain. Information within the MNIS

domain must be properly marked (A.UNMARKED_INFORMATION) to show its value (A.INFORMATION_VALUE), regardless of whether the originating country marked it. Furthermore, tools and resources must be available to permit the secure flow of information between domains (A.AUDIT_ANALYSIS, A.CONNECTIONS, O.AUDIT, and OE.MISUSE_DETECTION). Authentication of personnel (O.AUTHENTICATION and O.AUTHORIZED_USE) is performed prior to the release of sensitive information to a person in another domain.

P.DISTRIBUTION - *A Security Administrator will issue security relevant TOE hardware and software, and will maintain all records regarding distribution of these items.*

TOE Security Administrators must ensure proper configuration management (A.CONFIGURATION and A.TOE_OPERATION) of all security relevant hardware and software issued to any TOE user or administrator. This ensures that the TOE systems comply with applicable agreements and policies (A.COMPLY). Controlling the introduction of hardware and software minimizes the spread of malicious code (O.PROHIBIT_MALICIOUS_CODE). The TSE objective OE.DISTRIBUTION is directly derived from this policy.

P.DUE_CARE - *The level of security afforded the IT system must be in accordance with what is considered prudent by the Command's accrediting authority. This authority will assure that the organization's IT systems are implemented, maintained, and operated in a manner that represents due care and diligence with respect to usage issues and risks to the MNIS.*

Due care is related to almost every security assumption and objective. The sponsoring Command, the partner nations, and the TOE personnel (A.PERSONNEL_TRUST, A.COMPLY, A.CLEARANCE, A.POLICY_MNIS, A.SPONSOR, A.TOE_USER, and A.TRAINED) must ensure that diligent care is taken to protect the MNIS and its information. Due care encompasses A.CONFIGURATION, A.LOGISTICS_SUPPORT, A.PHYSICAL_SECURITY, A.POLICY_US_REL-LAN, A.TOE_DESIGN, A.TOE_MAINTENANCE, A.TOE_OPERATION, A.TOE_USER_AUTHENTICATION, O.AUDIT, O.AUTHENTICATION, O.AUTHORIZED_USE, O.CROSS_DOMAIN_FILTERING, O.ERROR_REJECT, O.MANAGE, O.NON-REPUDIATION, O.PROHIBIT_MALICIOUS_CODE, O.PROTECT, O.PROTECT_EXT_COMMS, O.REACT, and O.RECOVERY. Also, the implementation of the TOE must provide the capability for TOE personnel to form ad hoc groups dynamically and must protect the privacy of information flow between group members (A.COI). Within the MNIS system high environment the system must support robust communications among personnel (A.MNIS_INFO_INTERNAL) with all unmarked information treated as "Multinational Secret" (A.MNIS_INFO_CLASSIFICATION, A.SYSTEM_HIGH, and A.UNMARKED_INFORMATION). Communications between the MNIS domain and other domains will be more limited to provide adequate protection from attack (e.g., viruses and other malicious code as well as inadvertent errors) (A.CONNECTIONS and A.TRANSEC_CRYPTO).

P.MNIS_ENVIRON_EXTERNAL_DISTRO - *Confidentiality and integrity protection must be applied to information transferred into and out of the MNIS environment.*

Most of the information flowing in and out of the MNIS domain (A.CONNECTIONS) is classified (A.INFORMATION_VALUE and A.UNMARKED_INFORMATION) and must be protected from both unauthorized disclosure and modification (A.CRYPTO_SUPPORT, A.TRANSEC_CRYPTO, O.PROTECT, and O.PROTECT_EXT_COMM). Auditing and a misuse detection system are vital security tools (O.AUDIT and OE.MISUSE_DETECTION).

P.MNIS_ENVIRON_INTERNAL_DISTRO - *The MNIS environment is a physically protected system high environment for Secret MNIS information. Transmission security is not required within the protected environment, but access controls are necessary.*

The sponsoring Command is responsible for the physical protection of the MNIS environment (A.PHYSICAL_SECURITY, A.TEMPEST, and O.PROTECT). Because of these physical protections, rich sharing of information and supporting services are permitted without the need for cryptographic protection (A.MNIS_INFO_ACCESSIBLE, A.MNIS_INFO_INTERNAL, and A.SYSTEM_HIGH). However, access control mechanisms (O.AUTHENTICATION and O.AUTHORIZED_USE) are still necessary to enforce basic need to know principles (A.SYSTEM_HIGH). Auditing and misuse detection remain vital to protect the MNIS environment (O.AUDIT, OE.MISUSE_DETECT, and O.PROHIBIT_MALICIOUS_CODE) and react to attacks (O.REACT).

P.MNIS_INFO_PROTECT - *All information processed or stored internal to the MNIS Information Domain will be protected as Secret with appropriate releasability caveats.*

The MNIS domain consists of classified command, control, and intelligence information prepared within the MNIS environment and/or released from the U.S. and the partner nations to execute the assigned military mission. All information will be protected (O.PROTECT) at the "Multinational Secret" level (A.SYSTEM_HIGH) in the MNIS domain and must be labeled and/or caveated appropriately (A.MNIS_INFO_CLASSIFICATION and A.UNMARKED_INFORMATION). Similarly, the TOE must protect the privacy of information used by ad hoc groups (A.COI). Robust auditing and misuse detection mechanisms alert administrators when MNIS personnel request access to information to which they are not entitled (O.AUDIT, O.AUTHORIZED_USE, and OE.MISUSE_DETECTION). The sponsoring Command ensures that personnel will protect passwords and other TOE security mechanisms (OE.PROTECT_SECRETS).

P.MNIS_INFO_RECIPIENTS - *U.S. and partner personnel and processes that are recipients of information transferred out of the MNIS Information Domain must be explicitly authorized to receive it.*

MNIS policies (A.POLICY_MNIS and A.POLICY_US_REL-LAN) require the protection (O.PROTECT) of information within the MNIS information domain, and between it and partner domains. Security mechanisms must adjudicate all transfers of information from the MNIS information domain to another (A.CONNECTIONS and O.CROSS_DOMAIN_FILTERING). The TOE must validate the identity (O.AUTHENTICATION) of external recipients of MNIS information to prohibit unintentional disclosure of MNIS information. These transfers must be audited (O.AUDIT) and techniques employed to prevent a user from repudiating such transfers (O.NON_REPUDIATION). The TSE must employ a misuse detection system for analyzing audit data (OE.MISUSE_DETECTION).

P.MNIS_INFO_SENDERS - *TOE users and processes must be explicitly authorized to transfer information outside the MNIS Information Domain.*

MNIS policies (A.POLICY_MNIS and A.POLICY_US_REL-LAN) require the protection (O.PROTECT) of information within the MNIS information domain, and between it and partner domains. Security mechanisms must adjudicate all transfers of information from the MNIS information domain to another (A.CONNECTIONS and O.CROSS_DOMAIN_FILTERING). The TOE must validate the identity (A.TOE_USER, O.AUTHORIZED_USE, and O.AUTHENTICATION) of MNIS personnel to ensure they are authorized to export MNIS information. These personnel are trained and trusted (A.TRAINED and A.PERSONNEL_TRUST) to prevent unauthorized export of MNIS information. These transfers must be audited (O.AUDIT) and techniques employed to prevent a user from repudiating such transfers (O.NON_REPUDIATION). The TSE must employ a misuse detection system for analyzing audit data (OE.MISUSE_DETECTION).

P.MNIS_INFO_SOURCES - *U.S. and partner personnel and processes that transfer information into the MNIS Information Domain must be explicitly authorized to do so.*

MNIS policies (A.POLICY_MNIS and A.POLICY_US_REL-LAN) require the protection (O.PROTECT) of information within the MNIS information domain, and between it and partner domains. Security mechanisms must adjudicate all transfers of information into the MNIS information domain (A.CONNECTIONS and O.CROSS_DOMAIN_FILTERING). The TOE must validate the identity (O.AUTHENTICATION) of external sources of information to prohibit the import of unauthorized or malicious information. These transfers must be audited (O.AUDIT) and techniques employed to prevent a source from repudiating such transfers (O.NON_REPUDIATION). The TSE must employ a misuse detection system for analyzing audit data (OE.MISUSE_DETECTION).

P.REJECT_PARTNER_INFO - *The TOE will check all information it receives from partner sources. It will return and not allow information into the MNIS information domain that it determines to be outside the bounds of negotiated partnership information agreements.*

All multinational partners must comply (A.COMPLY) with negotiated policies and procedures (A.CLEARANCE, A.CONNECTIONS, A.POLICY_MNIS, and A.SYSTEM_HIGH) regarding TOE operation. Information must carry classification markings (A.INFORMATION_VALUE, A.UNMARKED_INFORMATION, and A.MNIS_INFO_CLASSIFICATION) and other data that are required to enforce cross-domain protection policies (O.CROSS_DOMAIN_FILTERING, and O.PROHIBIT_MALICIOUS_CODE). The TOE must identify and return suspect information flowing into the domain (O.AUDIT and OE.MISUSE_DETECTION) to protect (O.PROTECT) itself and react to attacks (O.REACT).

P.REJECT_U.S._INFO - *The TOE will check all information it receives from U.S. sources. It will return and not allow information that it determines to be higher than Secret or not releasable, to be processed or stored within the MNIS Information Domain.*

The U.S. must comply (A.COMPLY) with its policies and procedures (A.CLEARANCE, A.CONNECTIONS, A.POLICY_MNIS, and A.SYSTEM_HIGH) regarding TOE operation. The U.S. Releasability Local Area Network provides a MNIS domain presence (A.POLICY_US_REL-LAN) within the sponsoring Command's facility. All U.S. classified information must carry appropriate markings (A.INFORMATION_VALUE, A.UNMARKED_INFORMATION, and A.MNIS_INFO_CLASSIFICATION) and other data that are required to enforce cross-domain protection policies (O.CROSS_DOMAIN_FILTERING and O.PROHIBIT_MALICIOUS_CODE). The TOE must identify (O.AUDIT) and return (O.REACT) information that is not allowed out of the U.S. information domain.

P.SECURITY_ADMIN_RESTRICTED - *Only authorized System Administrators, Security Administrators, and their representatives may administer or repair security mechanisms (e.g., the cross domain filtering function) in the TOE.*

The roles of system and security administrator and maintenance person (A.TOE_MAINTENANCE) are extremely critical to any IT environment such as the TOE (A.TOE_OPERATION). Sufficient authorized (O.AUTHENTICATION and O.AUTHORIZED_USE) administrator personnel (A.ADMIN_AVAILABLE) must be available to fill these roles. They must be well-trained (A.TRAINED) and trustworthy (A.PERSONNEL_TRUST) and they must comply (A.COMPLY) with all established policies and procedures (A.POLICY_MNIS and A.POLICY_US_REL-LAN). Additionally, the TOE must be designed and implemented to separate the administrator roles (OE.SPLIT_ADMIN, OE.SPLIT_ADMIN_SECURITY, and OE.SPLIT_ADMIN_SYSTEM) to protect the TOE against administrator misuse (O.AUDIT, OE.MISUSE_DETECTION, and O.NON-

REPUDIATION). The physical environment of the MNIS domain must be protected and secure (A.PHYSICAL_SECURITY).

P.USERS - *Only personnel authorized by the sponsoring U.S. Combatant Command, Service, or Agency may have access to or utilize TOE resources.*

TOE personnel must be well-trained (A.TRAINED), sponsored (A.TOE_USER and A.SPONSOR), properly cleared (A.CLEARANCE), and authenticated (O.AUTHORIZED_USE, A.TOE_USER_AUTHENTICATION, O.AUTHENTICATION) to use the TOE. All TOE users must comply (A.COMPLY) with rules and regulation regarding its use. Personnel must understand that the information in the MNIS domain is available for all users (A.SYSTEM_HIGH and A.DYNAMIC_PARTNERSHIP) within a need-to-know philosophy (A.COI). The TOE must guard against misuse (O.AUDIT and OE.MISUSE_DETECTION) to protect (O.PROTECT) the information of all the nations involved in the operation. It must not permit violators of MNIS domain policy to deny they have done so (O.NON-REPUDIATION).

6.2 Security Objectives Rationale

A table in Section 6.2.1 maps the TOE security objectives to the identified threats. Following the table, rationale is provided for the coverage of each TOE Security Objective. Similarly, Section 6.2.2 provides a mapping table and rationale for the non-IT security objectives.

6.2.1 IT Security Objectives Rationale

Table 6 lists all of the identified threats to TOE security that are associated with each security objective. The rationale for each security objective is presented below the table.

Table 6 - Map IT Security Objectives to Threats

Security Objectives	Threats
O.AUDIT	T.ACCESS_ELECTRONIC, T.ALARM_FAIL, T.AUDIT_FAIL, T.AUTHORIZATION_EXCEED, T.DENIAL_OF_SERVICE, T.DISASTER_ENVIRO, T.ERROR_ADMIN, T.ERROR_USER, T.IMPERSONATE, T.IMPORT_BAD, T.MALICIOUS_ADMIN, T.MALICIOUS_USER, T.POOR_ADMIN, T.POOR_BACKUP, T.POOR_TRAIN, T.REPUDIATE, T.TOE_FAIL
O.AUTHENTICATION	T.ACCESS_ELECTRONIC, T.ACCESS_PHYSICAL, T.AUTHORIZATION_EXCEED, T.IMPERSONATE, T.REPUDIATE
O.AUTHORIZED_USE	T.ACCESS_ELECTRONIC, T.ACCESS_PHYSICAL, T.AUTHORIZATION_EXCEED, T.IMPERSONATE, T.MALICIOUS_ADMIN, T.MALICIOUS_USER, T.REPUDIATE
O.CROSS_DOMAIN_FILTERING	T.ACCESS_ELECTRONIC, T.AUTHORIZATION_EXCEED, T.DENIAL_OF_SERVICE, T.IMPERSONATE, T.IMPORT_BAD
O.ERROR_REJECT	T.ACCESS_ELECTRONIC, T.ALARM_FAIL, T.AUDIT_FAIL, T.AUTHORIZATION_EXCEED, T.ERROR_ADMIN, T.ERROR_USER, T.IMPORT_BAD, T.POOR_ADMIN, T.POOR_TRAIN, T.TOE_FAIL

O.MANAGE	T.ALARM_FAIL, T.AUDIT_FAIL, T.DISASTER_ENVIRO, T.ERROR_ADMIN, T.ERROR_USER, T.POOR_ADMIN, T.POOR_BACKUP, T.POOR_TRAIN
O.NON-REPUDIATION	T.AUTHORIZATION_EXCEED, T.MALICIOUS_ADMIN, T.MALICIOUS_USER, T.REPUDIATE
O.PROHIBIT_MALICIOUS_CODE	T.ALARM_FAIL, T.AUDIT_FAIL, T.DENIAL_OF_SERVICE, T.IMPORT_BAD, T.MALICIOUS_ADMIN, T.MALICIOUS_USER
O.PROTECT	T.AUTHORIZATION_EXCEED, T.ERROR_ADMIN, T.ERROR_USER, T.MALICIOUS_ADMIN, T.MALICIOUS_USER, T.POOR_ADMIN, T.POOR_TRAIN
O.PROTECT_EXT_COMMS	T.ACCESS_ELECTRONIC, T.COMPROMISE_CRYPTO
O.REACT	T.ACCESS_ELECTRONIC, T.ACCESS_PHYSICAL, T.ALARM_FAIL, T.AUDIT_FAIL, T.COMPROMISE_CRYPTO, T.DENIAL_OF_SERVICE, T.DISASTER_ENVIRO, T.ERROR_ADMIN, T.ERROR_USER, T.IMPERSONATE, T.IMPORT_BAD, T.MALICIOUS_ADMIN, T.MALICIOUS_USER, T.POOR_ADMIN, T.POOR_TRAIN, T.TOE_FAIL
O.RECOVERY	T.COMPROMISE_CRYPTO, T.DENIAL_OF_SERVICE, T.DISASTER_ENVIRO, T.ERROR_ADMIN, T.ERROR_USER, T.IMPORT_BAD, T.MALICIOUS_ADMIN, T.MALICIOUS_USER, T.POOR_ADMIN, T.POOR_BACKUP, T.POOR_IMPLEMENTATION, T.POOR_TRAIN, T.TOE_FAIL
O.TOE_FAILSAFE	T.COMPROMISE_CRYPTO, T.DISASTER_ENVIRO, T.POOR_IMPLEMENTATION, T.TOE_FAIL

O.AUDIT - *The TOE will monitor and generate accurate audit records of security relevant events.*

An accurate audit trail is necessary to detect a number of malicious threats to the TOE (T.ACCESS_ELECTRONIC, T.ALARM_FAIL, T.AUTHORIZATION_EXCEED, T.DENIAL_OF_SERVICE, T.IMPERSONATE, T.IMPORT_BAD, T.MALICIOUS_ADMIN, T.MALICIOUS_USER, and T.REPUDIATE). The audit trail will also help recover from non-malicious activity and certain types of errors (T.DISASTER_ENVIRO, T.ERROR_ADMIN, T.ERROR_USER, T.POOR_ADMIN, T.POOR_BACKUP, T.POOR_TRAIN, and T.TOE_FAIL). Finally, an easy-to-use audit trail reduces the threat of an audit failure (T.AUDIT_FAIL).

O.AUTHENTICATION - *The TOE must authenticate the identity of each user and administrator prior to granting access to, or use of, the TOE and its resources in accordance with their authorizations.*

Authentication will help ensure that unauthorized personnel do not have physical or electronic access to the TOE (T.ACCESS_ELECTRONIC, T.ACCESS_PHYSICAL, T.IMPERSONATE, and T.REPUDIATE). Authentication also helps to control access by authorized multinational personnel (T.AUTHORIZATION_EXCEED).

O.AUTHORIZED_USE - *The TOE must ensure that only uniquely identified users and administrators authorized by the sponsoring U.S. Command, Service, or Agency may utilize, administer or repair the TOE and its resources within the limits of their authorization.*

TOE personnel will be authorized to perform different functions (such as administration) and access different information and resources (including COI information). This security objective will prohibit unauthorized TOE access (T.AUTHORIZATION_EXCEED, T.IMPERSONATE, and T.REPUDIATE) and malicious access (T.ACCESS_ELECTRONIC, T.ACCESS_PHYSICAL, T.MALICIOUS_ADMIN, and T.MALICIOUS_USER).

O.CROSS_DOMAIN_FILTERING - *The TOE will include appropriate cross-domain filtering and authentication techniques between the MNIS Information Domain and external information domains, users, and processes. The TOE Cross-Domain Filtering function will allow only releasable information classified no higher than U.S.-Secret into the MNIS Information Domain.*

This security objective ensures that all personnel who transfer information in and out of the MNIS Information Domain are authorized to do so (T.ACCESS_ELECTRONIC, T.AUTHORIZATION_EXCEED, and T.IMPERSONATE) and that the content of all cross-domain transfers is valid and contains no malicious content (T.DENIAL_OF_SERVICE and T.IMPORT_BAD).

O.ERROR_REJECT - *The TOE must ensure that administrator or user error will not result in a violation of security policy, information compromise, a corruption of information integrity, or a degradation of secure TOE operation.*

The negative impact of mistakes (T.AUTHORIZATION_EXCEED, T.ERROR_ADMIN, T.ERROR_USER, T.POOR_ADMIN, and T.POOR_TRAIN) is increased in a multinational environment. Additionally, the TOE must be able to prevent errors that can affect secure TOE operation (T.ACCESS_ELECTRONIC, T.ALARM_FAIL, T.AUDIT_FAIL, T.IMPORT_BAD, and T.TOE_FAIL).

O.MANAGE - *The TOE must incorporate user friendly mechanisms to ensure secure administration of its operation.*

Easy to use security administrative functionality can counter some technical problems (T.ALARM_FAIL, T.AUDIT_FAIL, and T.POOR_BACKUP), human mistakes (T.ERROR_ADMIN, T.ERROR_USER, T.POOR_ADMIN, and T.POOR_TRAIN), and some environmental disasters (T.DISASTER_ENVIRO).

O.NON-REPUDIATION - *The TOE must accurately and dependably attribute actions performed by authorized users or administrators.*

Accurate attribution ensures that TOE users and administrators who attempt unauthorized TOE access (T.AUTHORIZATION_EXCEED, T.MALICIOUS_ADMIN, and T.MALICIOUS_USER) cannot deny (T.REPUDIATE) their unauthorized activity.

O.PROHIBIT_MALICIOUS_CODE - *The TOE must detect and prohibit attempts to introduce unauthorized or malicious code or applications into the TOE.*

Malicious code must be detected and neutralized whether imported from outside of the TOE (T.DENIAL_OF_SERVICE and T.IMPORT_BAD) or introduced by TOE personnel (T.MALICIOUS_ADMIN and T.MALICIOUS_USER), including malicious code that is designed to alter the audit trail (T.AUDIT_FAIL) or hinder TOE alarm operation (T.ALARM_FAIL).

O.PROTECT - *The TOE must protect against authorized users and administrators compromising information or degrading the secure operation of the TOE.*

The totality of the TOE security mechanisms must be able to provide sufficient protection to ensure continuing secure operation of the TOE. As noted above and below, this includes malicious activity (T.AUTHORIZATION_EXCEED, T.MALICIOUS_ADMIN, and T.MALICIOUS_USER) and mistakes by TOE personnel (T.ERROR_ADMIN, T.ERROR_USER, T.POOR_ADMIN, and T.POOR_TRAIN).

O.PROTECT_EXT_COMMS - *The TOE must include confidentiality and integrity protection between physically distributed environments of the TOE and between the TOE and partner environments.*

Data transmission between secure facilities must not provide unauthorized electronic access to the TOE (T.ACCESS_ELECTRONIC) or the ability to compromise data confidentiality (T.COMPROMISE_CRYPTO).

O.REACT - *The TOE will react to misuse detection analysis that is performed within the TSE and alert TOE administrators (e.g., detected viruses, unauthorized use, or audit file "full" conditions).*

The TOE must be able to respond to external threats (T.ACCESS_ELECTRONIC, T.ACCESS_PHYSICAL, T.COMPROMISE_CRYPTO, T.DENIAL_OF_SERVICE, T.DISASTER_ENVIRO, and T.IMPORT_BAD) and internal threats (T.ERROR_ADMIN, T.ERROR_USER, T.IMPERSONATE, T.MALICIOUS_ADMIN, T.MALICIOUS_USER, T.POOR_ADMIN, and T.POOR_TRAIN). The TOE must be able to respond to foreseeable problems that might cause TOE failure (T.ALARM_FAIL, T.AUDIT_FAIL, and T.TOE_FAIL).

O.RECOVERY - *The TOE must include mechanisms and implement predefined procedures to ensure that it is restored to a secure operational state following recovery from system failure.*

The TOE must be designed to automatically return to secure operation after certain kinds of attacks (T.COMPROMISE_CRYPTO, T.DENIAL_OF_SERVICE, T.IMPORT_BAD, T.MALICIOUS_ADMIN, and T.MALICIOUS_USER) and external problems (T.DISASTER_ENVIRO). Also, the TOE must be able to recover from internal system errors (T.POOR_BACKUP, T.POOR_IMPLEMENTATION, and T.TOE_FAIL) and personnel mistakes (T.ERROR_ADMIN, T.ERROR_USER, T.POOR_ADMIN, and T.POOR_TRAIN).

O.TOE_FAILSAFE - *The TOE must immediately react to specified security critical events and enter a secure state.*

Notwithstanding the goal of O.RECOVERY, the TOE design might not be able to recover from all events and attacks. In those cases where secure recovery is not possible, perhaps due to an overwhelming disaster (T.DISASTER_ENVIRO), substantial installation or maintenance error (T.POOR_IMPLEMENTATION), or other significant failure (T.TOE_FAIL), the TOE must enter a secure mode pending administrator intervention. When secure external connectivity is lost (T.COMPROMISE_CRYPTO), the cryptographic mechanisms must enter a secure mode.

6.2.2 Non-IT Objectives Rationale

Table 7 lists all of the identified threats to TOE security that are associated with each non-IT security objective. The rationale for each non-IT security objective is presented below the table.

Table 7 - Map Non-IT Security Objectives to Threats

Non-IT Security Objectives	Threats
OE.ACCESS_PHYSICAL	T.ACCESS_PHYSICAL, T.ALARM_FAIL
OE.AVAILABILITY_OF_SERVICE	T.DENIAL_OF_SERVICE, T.DISASTER_ENVIRO, T.TOE_FAIL
OE.BACKUP	T.DISASTER_ENVIRO, T.POOR_BACKUP, T.TOE_FAIL
OE.DISTRIBUTION	T.ACCESS_ELECTRONIC, T.ACCESS_PHYSICAL, T.POOR_ADMIN
OE.DUE_CARE	T.ALARM_FAIL, T.AUDIT_FAIL, T.COMPROMISE_CRYPTO, T.DISASTER_ENVIRO, T.ERROR_ADMIN, T.POOR_ADMIN, T.POOR_BACKUP, T.POOR_IMPLEMENTATION, T.POOR_TRAIN
OE.GOOD_ADMIN	T.ACCESS_ELECTRONIC, T.ALARM_FAIL, T.AUDIT_FAIL, T.DENIAL_OF_SERVICE, T.ERROR_ADMIN, T.IMPORT_BAD, T.POOR_ADMIN, T.POOR_BACKUP
OE.MISUSE_DETECTION	T.ALARM_FAIL, T.AUDIT_FAIL, T.AUTHORIZATION_EXCEED, T.DENIAL_OF_SERVICE, T.ERROR_ADMIN, T.ERROR_USER, T.MALICIOUS_ADMIN, T.MALICIOUS_USER, T.POOR_ADMIN, T.POOR_TRAIN, T.REPUDIATE
OE.PROTECT_SECRETS	T.ACCESS_ELECTRONIC, T.COMPROMISE_CRYPTO, T.IMPERSONATE
OE.SPLIT_ADMIN	T.AUTHORIZATION_EXCEED, T.ERROR_ADMIN, T.MALICIOUS_ADMIN, T.POOR_ADMIN

Non-IT Security Objectives	Threats
OE.SPLIT_ADMIN_SECURITY	T.AUTHORIZATION_EXCEED, T.ERROR_ADMIN, T.MALICIOUS_ADMIN, T.POOR_ADMIN
OE.SPLIT_ADMIN_SYSTEM	T.AUDIT_FAIL, T.AUTHORIZATION_EXCEED, T.ERROR_ADMIN, T.MALICIOUS_ADMIN, T.POOR_ADMIN

OE.ACCESS_PHYSICAL - *The TSE must include mechanisms and procedures that ensure the physical protection of the TOE from unauthorized agents.*

The TOE must be physically secure from unauthorized access (T.ACCESS_PHYSICAL) even in the event that some alarms fail to activate (T.ALARM_FAIL).

OE.AVAILABILITY_OF_SERVICE - *The TSE will detect attempts to deny TOE information and services to authorized users and administrators and will respond appropriately.*

The TOE must be protected from external influences (T.DENIAL_OF_SERVICE and T.DISASTER_ENVIRO) that could cause TOE failure (T.TOE_FAIL).

OE.BACKUP - *The TSE must ensure that adequate system backups are regularly performed in accordance with TOE policy and procedures.*

For the TOE to recover after a failure (T.TOE_FAIL), including externally induced failures (T.DISASTER_ENVIRO), the backup files must not be out-of-date or incomplete (T.POOR_BACKUP).

OE.DISTRIBUTION - *TSE procedures must ensure that TOE administrators issue security relevant TOE hardware and software to appropriate personnel, maintain inventory records of these items, and track the return or disposal of these items.*

Poor management and control of security assets (T.POOR_ADMIN), such as badges, security tokens, and software updates, may lead to unauthorized TOE access (T.ACCESS_ELECTRONIC and T.ACCESS_PHYSICAL).

OE.DUE_CARE - *Administrators will periodically ensure that the implementation, maintenance, and approved operating procedures for the TOE represent due care and diligence with respect to risks and threats, and that they comply with the organization's accrediting authority.*

Every aspect of TOE administration must demonstrate due care. Administrators must be properly trained (T.POOR_TRAIN) to minimize their errors (T.ERROR_ADMIN, T.POOR_ADMIN, and T.POOR_BACKUP) and to minimize TOE degradation (T.ALARM_FAIL, T.AUDIT_FAIL, and T.POOR_IMPLEMENTATION). Diligent administration can reduce the damage resulting from some external influences (T.COMPROMISE_CRYPTO and T.DISASTER_ENVIRO).

OE.GOOD_ADMIN - *Administrators of the TOE will periodically review configuration settings, ensure all current software patches are installed, and appropriately respond to alarms and audit analysis results.*

As a subset of OE.DUE_CARE, effective administrative practices reduce the effectiveness of malicious attacks (T.ACCESS_ELECTRONIC, T.DENIAL_OF_SERVICE, and T.IMPORT_BAD) and the likelihood of poor administrator performance (T.ERROR_ADMIN, T.POOR_ADMIN, and T.POOR_BACKUP). Administrators must always be ready to respond to TOE problems (T.ALARM_FAIL and T.AUDIT_FAIL).

OE.MISUSE_DETECTION - *The TSE must include the capability to interpret audit records, perform audit analysis, and generate audit alert for subsequent action.*

In a multinational environment, misuse detection must be pervasive to protect against insider and outside threats. Analysis and interpretation of TOE audit records must detect malicious activity (T.AUTHORIZATION_EXCEED, T.DENIAL_OF_SERVICE, T.MALICIOUS_ADMIN, and T.MALICIOUS_USER) and errors (T.ERROR_ADMIN, T.ERROR_USER, T.POOR_ADMIN, and T.POOR_TRAIN). Audit analysis must be able to individually identify users or administrators associated with every security-relevant event (T.REPUDIATE). Analysis mechanisms must be able to identify failure trends in the TOE audit (T.AUDIT_FAIL) and alarm systems (T.ALARM_FAIL).

OE.PROTECT_SECRETS - *Procedures must be established that will inhibit unauthorized agents from using social engineering techniques to gain security relevant information (e.g., passwords) about the TOE and the information it protects.*

The TOE and its cryptographic components must be protected (T.COMPROMISE_CRYPTO) from unauthorized electronic access (T.ACCESS_ELECTRONIC) by unauthorized personnel attempting to masquerade (T.IMPERSONATE) as authorized TOE personnel.

OE.SPLIT_ADMIN - *The TSE must include mechanisms to ensure that the administration of the TOE is appropriately split between the defined roles of TOE System and Security Administrators.*

To reduce the possibility for a TOE administrator to maliciously or erroneously affect TOE security (T.ERROR_ADMIN, T.MALICIOUS_ADMIN, and T.POOR_ADMIN), no individual TOE administrator will be given authorization to perform all TOE administrative functions. No TOE administrator will be able to authorize any TOE user or administrator to have access to all TOE administrative capabilities (T.AUTHORIZATION_EXCEED).

OE.SPLIT_ADMIN_SECURITY - *A Security Administrator interprets, maintains, and oversees site security policy and develops and implements procedures assuring secure operation of the TOE.*

To reduce the possibility for a TOE Security Administrator to degrade TOE security (T.ERROR_ADMIN, T.MALICIOUS_ADMIN, and T.POOR_ADMIN), they will be authorized to perform only Security Administrator duties when accessing the TOE via a TOE Security Administrator account. No individual TOE Security Administrator will be given authorization to perform TOE System Administrator functions (T.AUTHORIZATION_EXCEED).

OE.SPLIT_ADMIN_SYSTEM - *A System Administrator installs, configures, manages, and monitors the performance of the TOE, ensuring that the TOE complies with its evaluated configuration and conforms to applicable security policies.*

To reduce the possibility for a TOE System Administrator to degrade TOE security (T.ERROR_ADMIN, T.MALICIOUS_ADMIN, and T.POOR_ADMIN), they will be authorized to perform only system administrator duties when accessing the TOE via a TOE System Administrator account. No individual TOE System Administrator will be given authorization to perform security administrator functions (T.AUTHORIZATION_EXCEED).

6.3 Security Functional Requirements Rationale

The security functional requirements presented in this Protection Profile are mutually supportive and combine to meet the stated security objectives as shown in Table 8, below. The security requirements were derived from the MNIS Model according to the approach presented in Part 1 of the Common Criteria. The rationale for each functional requirement follows the table.

Table 8 - Mapping of Functional Requirements to Security Objectives

	O.AUDIT	O.AUTHENTICATION	O.AUTHORIZED_USE	O.CROSS_DOMAIN_FILTERING	O.ERROR_REJECT	O.MANAGE	O.NON-REPUDIATION	O.PROHIBIT_MALICIOUS_CODE	O.PROTECT	O.PROTECT_EXT_COMMS	O.REACT	O.RECOVERY	O.TOE_FAILSAFE	OE.ACCESS_PHYSICAL	OE.AVAILABILITY_OF_SERVICE	OE.BACKUP	OE.DISTRIBUTION	OE.DUE_CARE	OE.GOOD_ADMIN	OE.MISUSE_DETECTION	OE.PROTECT_SECRETS	OE.SPLIT_ADMIN	OE.SPLIT_ADMIN_SECURITY	OE.SPLIT_ADMIN_SYSTEM
FAU_ARP.1				X					X	X	X									X				
FAU_GEN.1	X																	X						
FAU_GEN.2	X						X																	
FAU_SAA.1										X										X				
FAU_SAA.2					X				X		X				X					X				
FAU_SAA.3					X				X		X				X					X				
FAU_SAR.1	X		X			X												X						
FAU_SAR.2	X		X			X												X						

	O.AUDIT	O.AUTHENTICATION	O.AUTHORIZED_USE	O.CROSS_DOMAIN_FILTERING	O.ERROR_REJECT	O.MANAGE	O.NON-REPUDIATION	O.PROHIBIT_MALICIOUS_CODE	O.PROTECT	O.PROTECT_EXT_COMMS	O.REACT	O.RECOVERY	O.TOE_FAILSAFE	OE.ACCESS_PHYSICAL	OE.AVAILABILITY_OF_SERVICE	OE.BACKUP	OE.DISTRIBUTION	OE.DUE_CARE	OE.GOOD_ADMIN	OE.MISUSE_DETECTION	OE.PROTECT_SECRETS	OE.SPLIT_ADMIN	OE.SPLIT_ADMIN_SECURITY	OE.SPLIT_ADMIN_SYSTEM
FAU_SAR.3	X		X			X												X	X					
FAU_SEL.1	X					X												X						
FCO_NRO.1		X	X				X																	
FCS_CKM.1										X											X			
FCS_CKM.2										X											X			
FCS_CKM.4										X											X			
FCS_COP.1										X											X			
FDP_ACC.2			X				X															X		
FDP_ACF.1			X				X																	
FDP_DAU.1		X	X																	X				
FDP_ETC.2			X	X																				
FDP_IFC.1		X	X																					
FDP_IFC.2				X				X											X			X		
FDP_IFF.1		X	X	X			X																	
FDP_IFF.2	X	X	X	X			X																	
FDP_IFF.3				X	X																			
FDP_ITC.2			X	X																				
FDP_ITT.2	X		X																		X	X		
FDP_RIP.1			X						X												X	X		
FDP_RIP.2									X												X			
FDP_ROL.1			X									X								X				
FIA_AFL.1		X			X				X				X							X				
FIA_ATD.1	X	X	X	X			X													X		X	X	X
FIA_SOS.1		X							X												X			
FIA_UAU.2	X		X				X													X				
FIA_UAU.4		X	X				X			X								X			X			
FIA_UAU.5		X	X				X		X								X				X			
FIA_UAU.6		X	X				X		X												X			
FIA_UAU.7		X	X				X		X												X			
FIA_UID.2	X	X	X																					
FIA_USB.1	X	X	X	X			X		X					X				X		X		X	X	X
FMT_MOF.1	X		X			X	X		X									X	X			X	X	X
FMT_MSA.1			X	X																			X	
FMT_MSA.2					X				X									X			X			
FMT_MSA.3			X															X						
FMT_MTD.1	X		X		X													X						
FMT_MTD.2	X		X		X	X						X						X	X					X
FMT_MTD.3					X	X			X									X	X					
FMT_REV.1			X	X		X			X					X				X	X			X	X	X
FMT_SMR.1		X	X				X															X	X	X
FMT_SMR.2		X	X				X															X	X	X

	O.AUDIT	O.AUTHENTICATION	O.AUTHORIZED_USE	O.CROSS_DOMAIN_FILTERING	O.ERROR_REJECT		O.NON-REPUDIATION	O.PROHIBIT_MALICIOUS_CODE	O.PROTECT	O.PROTECT_EXT_COMMS	O.REACT		O.TOE_FAILSAFE	OE.ACCESS_PHYSICAL	OE.AVAILABILITY_OF_SERVICE	OE.BACKUP	OE.DISTRIBUTION		OE.GOOD_ADMIN	OE.MISUSE_DETECTION	OE.PROTECT_SECRETS	OE.SPLIT_ADMIN	OE.SPLIT_ADMIN_SECURITY	SYSTEM
FMT_SMR.3			X				X															X	X	X
FPR_UNO.4				X	X	X		X	X		X							X	X	X		X	X	X
FPT_AMT.1									X															
FPT_FLS.1					X	X		X	X		X	X			X	X				X				
FPT_ITI.1	X				X				X		X	X								X				
FPT_ITT.1					X				X		X	X												
FPT_ITT.3					X			X	X		X	X			X					X				
FPT_PHP.2					X				X	X	X			X			X			X				
FPT_RCV.2					X				X	X	X	X	X		X					X				
FPT_RPL.1			X		X		X		X		X									X	X	X		
FPT_RVM.1		X	X						X															
FPT_SEP.3			X		X			X													X	X	X	X
FPT_STM.1	X						X									X		X						
FPT_TDC.1			X		X				X											X				
FPT_TST.1						X		X	X									X		X				
FRU_FLT.1									X		X		X		X					X				
FRU_RSA.1			X	X		X			X											X				
FTA_MCS.1		X	X				X														X			
FTA_MCS.2			X																X			X	X	X
FTA_SSL.1		X	X				X		X				X											
FTA_SSL.2		X	X				X		X				X											
FTA_SSL.3									X				X		X									
FTA_TAB.1						X												X						
FTA_TAH.1			X						X									X		X				
FTA_TSE.1		X	X				X		X				X							X				
FTP_ITC.1			X						X									X						
FTP_TRP.1		X	X			X			X									X			X			

6.3.1 Class FAU: Security Audit

FAU_ARP.1 Security Alarms

This component applies to the Cross-Domain, Security Administration, and Transmission Security categories. All TOE capabilities that support Cross-Domain security enforcement, security administration, and transmission security must be able to detect potential security violations and take specific actions in response to the detection.

Objectives addressed: O.CROSS_DOMAIN_FILTERING, O.PROTECT, O.PROTECT_EXT_COMMS, O.REACT, and OE.MISUSE_DETECTION

FAU_GEN.1 Audit Data Generation
This component applies to all categories. Most of the TOE security functions depend on the generation of an accurate and complete audit record.
Objectives addressed: O.AUDIT and OE.DUE_CARE

FAU_GEN.2 User Identity Association
This component applies to all categories. Individual accountability is necessary for all audit events to provide for the identification of every person who is responsible for each event.
Objectives addressed: O.AUDIT, O.NON-REPUDIATION, and OE.DUE_CARE

FAU_SAA.1 Potential Violation Analysis
This component applies to the Transmission Security category. Although most of the audit analysis is performed in the TOE security environment, the sensitivity of cryptographic components requires that they be able to identify a subset of potential violations based on audit events.
Objectives addressed: O.PROTECT_EXT_COMMS and OE.MISUSE_DETECTION

FAU_SAA.2 Profile Based Anomaly Detection
This component applies to the Cross-Domain and Security Administration categories. The sensitivity of Cross-Domain security devices and security administration functions requires that these mechanisms keep a profile of individual user and administrator usage, as described in the Security Target. When the activity by a user or an administrator reaches a specified threshold, the TSF must respond as determined in the Security Target, even if no actual security violation has occurred.
Objectives addressed: O.ERROR_REJECT, O.PROTECT, O.REACT, OE.AVAILABILITY_OF_SERVICE, and OE.MISUSE_DETECTION

FAU_SAA.3 Simple Attack Heuristics
This component applies to the Cross-Domain and Security Administration categories. Similar to FAU_SAA.2, Profile Based Anomaly Detection, Cross-Domain security devices and security administration functions may be vulnerable to readily discernable attacks. These mechanisms must be able to identify these types of attack based on signature events, as described in the Security Target. When the signature event is detected, the TSF must respond as determined in the Security Target, even if no actual security violation has occurred.
Objectives addressed: O.ERROR_REJECT, O.PROTECT, O.REACT, OE.AVAILABILITY_OF_SERVICE, and OE.MISUSE_DETECTION

FAU_SAR.1 Audit Review
This component applies to the Security Administration category. Only TOE Security and System Administrators are to be authorized to review and archive the TOE audit records.
Objectives addressed: O.AUDIT, O.AUTHORIZED_USE, O.MANAGE, and OE.DUE_CARE

FAU_SAR.2 Restricted Audit Review
This component applies to the Security Administration category. Except for TOE Security and System Administrators, no other users are to be allowed access to the TOE audit records.
Objectives addressed: O.AUDIT, O.AUTHORIZED_USE, O.MANAGE, and OE.DUE_CARE

FAU_SAR.3 Selectable Audit Review
This component applies to the Security Administration category. This is a straightforward requirement to provide tools for authorized personnel (per FAU_SAR.1) to manually review TOE audit records.
Objectives addressed: O.AUDIT, O.AUTHORIZED_USE, O.MANAGE, OE.DUE_CARE, and OE.GOOD_ADMIN

FAU_SEL.1 Selective Audit
This component applies to the Cross-Domain and Security Administration categories. TOE Security Administrators must be able to tailor the audit record to include or exclude certain events and also to include or exclude all events from certain hosts.
Objectives addressed: O.AUDIT, O.MANAGE, and OE.DUE_CARE

6.3.2 Class FCO: Communication

FCO_NRO.1 Selective Proof of Origin
This component applies to the Cross-Domain and Security Administration categories. When these categories of TOE security functionality receive information from remote sources (such as data being transferred Cross-Domain or remote administration of the TOE), then proof of origin is required for the information that is received. This will allow the Cross-Domain guarding systems to authenticate the originator of information being transferred across the MNIS Information Domain boundary. It will also allow for remote administration of the TOE by authorized administrators.
Objectives addressed: O.AUTHENTICATION, O.AUTHORIZED_USE, and O.NON-REPUDIATION

6.3.3 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic Key Generation
This component applies to the Transmission Security category. The TOE cryptographic functions must provide sufficient strength to protect information classified Secret from unauthorized disclosure. This requirement does not apply to cryptographic functions used to control access to Community of Interest information within the MNIS Information Domain.
Objectives addressed: O.PROTECT_EXT_COMMS and OE.PROTECT_SECRETS

FCS_CKM.2 Cryptographic Key Distribution
This component applies to the Transmission Security category. The methods used to distribute TOE cryptographic keys must comply with the standards for protecting information classified

Secret. This requirement does not apply to key distribution used by functions that control access to Community of Interest information within the MNIS Information Domain.
Objectives addressed: O.PROTECT_EXT_COMMS and OE.PROTECT_SECRETS

FCS_CKM.4 Cryptographic Key Destruction
This component applies to the Transmission Security category. The methods used to destroy TOE cryptographic keys must comply with the standards for protecting information classified Secret. This requirement does not apply to key destruction used by functions that control access to Community of Interest information within the MNIS Information Domain.
Objectives addressed: O.PROTECT_EXT_COMMS and OE.PROTECT_SECRETS

FCS_COP.1 Cryptographic Operation
This component applies to the Transmission Security category and is incorporated by reference as discussed in Section 5.2.4.
Objectives addressed: O.PROTECT_EXT_COMMS and OE.PROTECT_SECRETS

6.3.4 Class FDP: User Data Protection

FDP_ACC.2 Complete Access Control
This component applies to the Access Control, Cross-Domain, and Security Administration categories. All TOE security components shall enforce a mandatory access control policy on requests to access TOE resources. This ensures that unauthorized personnel do not have access to the TOE, that TOE users do not have access to TOE administrator resources, and that TOE roles are kept separate.
Objectives addressed: O.AUTHORIZED_USE, O.NON-REPUDIATION, and OE.SPLIT_ADMIN

FDP_ACF.1 Security Attribute Based Access Control
This component applies to the Access Control, Cross-Domain, and Security Administration categories. It lists the minimum attributes necessary to enforce TOE security policies and minimum rules for enforcing access control. The Security Target may list additional attributes and rules.
Objectives addressed: O.AUTHORIZED_USE and O.NON-REPUDIATION

FDP_DAU.1 Basic Data Authentication
This component applies to the Cross-Domain, Security Administration, and Transmission Security categories. The TOE must check the integrity of information used to validate Cross-Domain transfers, information used to enforce TOE security policies, and other information listed in the Security Target. This check increases the likelihood that policy enforcement mechanisms perform properly.
Objectives addressed: O.AUTHENTICATION, O.AUTHORIZED_USE, and OE.MISUSE_DETECTION

FDP_ETC.2 Export of User Data with Security Attributes

This component applies to the Cross-Domain category. TOE user data will most likely be classified because it is associated with the command and control of multinational forces. Cross-Domain data export mechanisms will enforce the Cross-Domain security policy based on the content of the data and on the data security attributes.

Objectives addressed: O.AUTHORIZED_USE and O.CROSS_DOMAIN_FILTERING

FDP_IFC.1 Subset Information Flow Control

This component applies to the Access Control category. This requirement is related to the flow of Community of Interest (COI) data within the MNIS Information Domain. Medium robustness mechanisms are sufficient to separate COI data from the rest of the MNIS data.

Objectives addressed: O.AUTHENTICATION and O.AUTHORIZED USE

FDP_IFC.2 Complete Information Flow Control

This component applies to the Cross-Domain and Security Administration categories. All information that flows across the MNIS Information Domain boundary must comply with the TOE Cross-Domain security policy. All TOE security administration functions must comply with the TOE access control policies, including split administration and mandatory access controls.

Objectives addressed: O.CROSS_DOMAIN_FILTERING, O.PROHIBIT_MALICIOUS_CODE, OE.GOOD_ADMIN, and OE.SPLIT_ADMIN

FDP_IFF.1 Simple Security Attributes

This component applies to the Security Administration and Transmission Security categories. This requirement specifies the user attributes and the data attributes needed to enforce TOE security policies.

Objectives addressed: O.AUTHENTICATION, O.AUTHORIZED USE, O.CROSS_DOMAIN_FILTERING, and O.NON-REPUDIATION

FDP_IFF.2 Hierarchical Security Attributes

This component applies to the Access Control and Cross-Domain categories.

a. In the case of the Access Control category, the TSF uses hierarchical attributes to control access to COI information.
b. In the case of the Cross-Domain category, the TSF uses hierarchical attributes to enforce cross-domain policies.

Objectives addressed: O.AUDIT, O.AUTHENTICATION, O.AUTHORIZED USE, O.CROSS_DOMAIN_FILTERING, and O.NON-REPUDIATION

FDP_IFF.3 Limited Illicit Information Flows

This component applies to the Cross-Domain Filtering category. The Cross-Domain security policy enforcement mechanism must be able to restrict the amount of unauthorized flows to less than a specified limit. The numerical value of this limit is not specified in this PP and must be provided in the Security Target.

Objectives addressed: O.CROSS_DOMAIN_FILTERING and O.ERROR_REJECT

FDP_ITC.2 Import of User Data with Security Attributes
This component applies to the Cross-Domain Filtering category. TOE user data will most likely be classified because it is associated with the command and control of multinational forces. Cross-Domain data import mechanisms will enforce the Cross-Domain security policy based on the data security attributes and the content of the data.
Objectives addressed: O.AUTHORIZED_USE and O.CROSS_DOMAIN_FILTERING

FDP_ITT.2 Transmission Separation by Attribute
This component applies to the Access Control category. Although the MNIS Information Domain is a system-high classified domain, the TOE must control access to certain types of information. Unauthorized TOE personnel must be prohibited from access to audit data, data used for TOE security and system administration, COI data, and other data whose attributes are given in the Security Target.
Objectives addressed: O.AUDIT, O.AUTHORIZED_USE, OE.PROTECT_SECRETS, and OE.SPLIT_ADMIN

FDP_RIP.1 Subset Residual Information Protection
This component applies to the Access Control and Security Administration categories. To prohibit the unauthorized disclosure of information, the TOE must ensure that information cannot be recovered from reused objects that stored or processed COI data, administration data, and other data listed in the Security Target.
Objectives addressed: O.AUTHORIZED_USE, O.PROTECT, OE.PROTECT_SECRETS, and OE.SPLIT_ADMIN

FDP_RIP.2 Full Residual Information Protection
This component applies to the Cross-Domain Filtering category. To prohibit the unauthorized disclosure of information, the TOE must ensure that information cannot be recovered from reused objects in Cross-Domain enforcement systems.
Objectives addressed: O.PROTECT and OE.PROTECT_SECRETS

FDP_ROL.1 Basic Rollback
This component applies to the Security Administration category. Poor administrator operations may have a broad impact on TOE security. Therefore, rollback may be necessary to restore proper TOE operations.
Objectives addressed: O.AUTHORIZED_USE, O.RECOVERY, and OE.MISUSE_DETECTION

6.3.5 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication Failure Handling
This component applies to all categories. It ensures that an upper bound exists on the number of attempts to use a TOE authentication mechanism. After the limit of unsuccessful login attempts

has been reached, the TOE no longer allows any more login or authentication attempts for that user and alerts TOE administrators to intervene.
Objectives addressed: O.AUTHENTICATION, O.ERROR_REJECT, O.PROTECT, O.TOE_FAILSAFE, and OE.MISUSE_DETECTION

FIA_ATD.1 User Attribute Definition
This component applies to the Access Control, Cross-Domain Filtering, and Security Administration categories and provides a list of attributes used by the TOE to distinguish users from each other. The TSF uses these attributes to enforce applicable security policies.
Objectives addressed: O.AUDIT, O.AUTHENTICATION, O.AUTHORIZED_USE, O.CROSS_DOMAIN_FILTERING, O.NON-REPUDIATION, OE.MISUSE_DETECTION, OE.SPLIT_ADMIN, OE.SPLIT_ADMIN_SECURITY, and OE.SPLIT_ADMIN_SYSTEM

FIA_SOS.1 Verification of Secrets
This component applies to the Access Control and Cross-Domain Filtering categories and places minimum characteristics for the quality of secrets used in the TOE, primarily the quality of TOE user and administrator passwords. The Security Target may supplement the characteristics to improve the quality of secrets.
Objectives addressed: O.AUTHENTICATION, O.PROTECT, and OE.PROTECT_SECRETS

FIA_UAU.2 Timing of Authentication
This component applies to all categories and requires successful user and administrator authentication before allowing any other use of the TOE. This is a basic requirement for many TOE security functions, such as non-repudiation, auditing, and authorization.
Objectives addressed: O.AUDIT, O.AUTHORIZED_USE, O.NON-REPUDIATION, and OE.MISUSE_DETECTION

FIA_UAU.4 Single-Use Authentication Mechanisms
This component applies to the Transmission Security category. The TOE will ensure that cryptographic keys are not accidentally reused beyond their intended period.
Objectives addressed: O.AUTHENTICATION, O.AUTHORIZED_USE, O.NON-REPUDIATION, O.PROTECT_EXT_COMMS, OE.DUE_CARE, and OE.PROTECT_SECRETS

FIA_UAU.5 Multiple Authentication Mechanisms
This component applies to the Security Administration category. It ensures that a combination of a password and a token are used for authentication of remote TOE administrators via an external network.
Objectives addressed: O.AUTHENTICATION, O.AUTHORIZED_USE, O.NON-REPUDIATION, O.PROTECT, OE.DISTRIBUTION, and OE.PROTECT_SECRETS

FIA_UAU.6 Re-Authenticating
This component applies to the Access Control and Security Administration categories. After the TOE locks an active session, the user or administrator must reauthenticate prior to regaining access to the TOE. This ensures that a different individual assigned to the multinational partnership cannot make use of the locked session.
Objectives addressed: O.AUTHENTICATION, O.AUTHORIZED_USE, O.NON-REPUDIATION, O.PROTECT, and OE.PROTECT_SECRETS

FIA_UAU.7 Protected Authentication Feedback
This component applies to the Access Control category. During authentication, the TOE must not display passwords on any terminal or workstation. This protects the password from being read and used by another person nearby.
Objectives addressed: O.AUTHENTICATION, O.AUTHORIZED_USE, O.NON-REPUDIATION, O.PROTECT, and OE.PROTECT_SECRETS

FIA_UID.2 User identification before any action
This component applies to all categories. It ensures that before any action occurs on behalf of a user, the user's is identified to the TOE.
Objectives addressed: O.AUDIT, O.AUTHENTICATION, and O.AUTHORIZED_USE

FIA_USB.1 User-Subject Binding
This component applies to the Access Control, Cross-Domain, and Security Administration categories. In a multinational environment with Cross-Domain data transfers, the TOE must individually attribute all activities performed by or on behalf of any user.
Objectives addressed: O.AUDIT, O.AUTHENTICATION, O.AUTHORIZED_USE, O.CROSS_DOMAIN_FILTERING, O.NON-REPUDIATION, O.PROTECT, OE.ACCESS_PHYSICAL, OE.DUE_CARE, OE.MISUSE_DETECTION, OE.SPLIT_ADMIN, OE.SPLIT_ADMIN_SECURITY, and OE.SPLIT_ADMIN_SYSTEM

6.3.6 Class FMT: Security Management

FMT_MOF.1 Management of Security Functions Behavior
This component applies to the Access Control, Cross-Domain Filtering, and Security Administration categories. Only TOE Security Administrators will be able to use, control, and change TOE security functions, including audit generation, authentication, attribute assignments, and other functions listed in the Security Target. All other users, including TOE System Administrators, must not be allowed to modify TOE security functions.
Objectives addressed: O.AUDIT, O.AUTHORIZED_USE, O.MANAGE, O.NON-REPUDIATION, O.PROTECT, OE.DUE_CARE, OE.GOOD_ADMIN, OE.SPLIT_ADMIN, OE.SPLIT_ADMIN_SECURITY, and OE.SPLIT_ADMIN_SYSTEM

FMT_MSA.1 Management of Security Attributes

This component applies to the Access Control and Cross-Domain Filtering categories and restricts the ability to change the necessary security information used during access control and during Cross-Domain policy enforcement to TOE Security Administrators.

Objectives addressed: O.AUTHORIZED_USE, O.CROSS_DOMAIN_FILTERING, and OE.SPLIT_ADMIN_SECURITY

FMT_MSA.2 Secure Security Attributes

This component applies to the Access Control, Security Administration, and Transmission Security categories and affects the default selection of security attributes and the range of allowable values for security attributes. The TOE is to reject the assignment of any security attributes that are determined to create an unsecure condition in the TOE. For example, the TOE must reject blank passwords.

Objectives addressed: O.ERROR_REJECT, O.PROTECT, OE.DUE_CARE, and OE.PROTECT_SECRETS

FMT_MSA.3 Static Attribute Initialization

This component applies to the Access Control, Cross-Domain, and Security Administration categories. The TOE must enforce restrictive default values for attributes used to enforce TOE security function policies. For example, upon creation of a TOE user account, the default value will be that the user lacks authorization to export information outside of the MNIS Information Domain.

Objectives addressed: O.AUTHORIZED_USE and OE.DUE_CARE

FMT_MTD.1 Management of TSF Data

This component applies to the Access Control, Cross-Domain Filtering, and Security Administration categories. The Security Target may specify access and management restrictions on additional types of TSF data.

a. For the Access Control category, this component ensures that users and TOE System Administrators are prohibited from changing the user security attributes and object security attributes used by the TSF to enforce security policies. Only TOE Security Administrators are authorized to query or manage these attributes.
b. For the Cross-Domain and Security Administration categories, this component ensures that users are not allowed to query the audit trail and additional information, if specified in the Security Target. This restricts users from determining what activities the TOE auditing capability is recording. Only TOE Security and System Administrators are authorized to query the audit trail.

Objectives addressed: O.AUDIT, O.AUTHORIZED_USE, O.ERROR_REJECT, and OE.DUE_CARE

FMT_MTD.2 Management of Limits on TSF Data

This component applies to the Security Administration category. It ensures that users and TOE Security Administrators are not allowed to manage size of backup files, audit storage files, and

additional data limits if specified in the Security Target. This restricts users and TOE Security Administrators from setting storage limits beyond what is physically available in the TOE or TSE. Only TOE System Administrators are authorized to set these size limits.
Objectives addressed: O.AUDIT, O.AUTHORIZED_USE, O.ERROR_REJECT, O.MANAGE, O.RECOVERY, OE.DUE_CARE, OE.GOOD_ADMIN, and OE.SPLIT_ADMIN_SYSTEM.

FMT_MTD.3 Secure TSF Data
This component applies to the Security Administration and Transmission Security categories. It limits the range of allowable values for TSF data attributes so that the TOE will reject the assignment of any TSF data values that are determined to create an unsecure condition in the TOE. For example, the TOE must reject setting the size of the audit files to zero.
Objectives addressed: O.ERROR_REJECT, O.MANAGE, O.PROTECT, OE.DUE_CARE, and OE.GOOD_ADMIN

FMT_REV.1 Revocation
This component applies to the Access Control and Security Administration categories. Only TOE Security Administrators will be authorized to revoke certain TOE security attributes, especially those used to enforce Cross-Domain security policies. No users or TOE System Administrators will be authorized to do so.
Objectives addressed: O.AUTHORIZED_USE, O.CROSS_DOMAIN_FILTERING, O.MANAGE, O.PROTECT, OE.ACCESS_PHYSICAL, OE.DUE_CARE, OE.GOOD_ADMIN, OE.SPLIT_ADMIN, OE.SPLIT_ADMIN_SECURITY, and OE.SPLIT_ADMIN_SYSTEM

FMT_SMR.1 Security Roles
This component applies to the Cross-Domain and Transmission Security categories. The TOE must maintain separate security administrator and system administrator roles. Separate roles will exist for personnel authorized to manage cryptographic components.
Objectives addressed: O.AUTHENTICATION, O.AUTHORIZED_USE, O.NON-REPUDIATION, OE.SPLIT_ADMIN, OE.SPLIT_ADMIN_SECURITY, and OE.SPLIT_ADMIN_SYSTEM

FMT_SMR.2 Restrictions on Security Roles
This component applies to the Access Control and Security Administration categories. A person logged in as a TOE Security Administrator cannot simultaneously log in as a TOE System Administrator, and vice versa.
Objectives addressed: O.AUTHENTICATION, O.AUTHORIZED_USE, O.NON-REPUDIATION, OE.SPLIT_ADMIN, OE.SPLIT_ADMIN_SECURITY, and OE.SPLIT_ADMIN_SYSTEM

FMT_SMR.3 Assuming Roles
This component applies to the Access Control, Cross-Domain, and Security Administration categories. An authorized TOE administrator is expected to also have a TOE user account. Any

individual with more than one TOE role must explicitly sign on to the proper account for that role and then sign off when finished with that role.
Objectives addressed: O.AUTHORIZED_USE, O.NON-REPUDIATION, OE.SPLIT_ADMIN, OE.SPLIT_ADMIN_SECURITY, and OE.SPLIT_ADMIN_SYSTEM

6.3.7 Class FPR: Privacy

FPR_UNO.4 Authorized User Observability
This component applies to the Security Administration category. To provide for proper TOE security, all TOE Security Administrators are authorized to view all COI information being protected by the TOE and all data stored or processed in Cross-Domain enforcement systems.
Objectives addressed: O.CROSS_DOMAIN_FILTERING, O.ERROR_REJECT, O.MANAGE, O.PROHIBIT_MALICIOUS_CODE, O.PROTECT, O.REACT, OE.DUE_CARE, OE.GOOD_ADMIN, OE.MISUSE_DETECTION, OE.SPLIT_ADMIN, OE.SPLIT_ADMIN_SECURITY, and OE.SPLIT_ADMIN_SYSTEM

6.3.8 Class FPT: Protection of the TOE Security Functions

FPT_AMT.1 Abstract Machine Testing
This component applies to the Access Control, Cross-Domain Filtering, and Security Administration categories. There is not a firm justification for this component. However, it is a dependency of FPT_TST.1, so it must be included in this PP.
Objectives addressed: O.PROTECT

FPT_FLS.1 Failure with Preservation of Secure State
This component applies to the Access Control, Cross-Domain Filtering, and Security Administration categories. The TOE must be able to withstand certain incidents without a reduction of TOE security. These incidents include a loss of electrical power or network connectivity, TOE detection and control of minor security incidents, and other failures listed in the Security Target.
Objectives addressed: O.ERROR_REJECT, O.MANAGE, O.PROHIBIT_MALICIOUS_CODE, O.PROTECT, O.REACT, O.RECOVERY, OE.AVAILABILITY_OF_SERVICE, OE.BACKUP, and OE.MISUSE_DETECTION

FPT_ITI.1 Inter-TSF Detection of Modification
This component applies to the Security Administration category. The TOE must be able to detect any modification of TOE security data (such as audit data) as it transits the TOE, to allow for retransmission or error correction. Additionally, TOE audit information will help identify and eliminate the source of modification.
Objectives addressed: O.AUDIT, O.ERROR_REJECT, O.PROTECT, O.REACT, O.RECOVERY, and OE.MISUSE_DETECTION

FPT_ITT.1 Basic Internal TSF Data Transfer Protection
This component applies to the Cross-Domain Filtering and Security Administration categories. The TOE must be able to protect data from modification as it transits the TOE, to allow for retransmission or error correction.
Objectives addressed: O.ERROR_REJECT, O.PROTECT, O.REACT, and O.RECOVERY

FPT_ITT.3 TSF Data Integrity Monitoring
This component applies to the Security Administration category. The TOE must be able to detect any modification, substitution, or deletion of TOE security data (such as audit data) during transmission between parts of the TOE to ensure that security functionality is not diminished.
Objectives addressed: O.ERROR_REJECT, O.PROHIBIT_MALICIOUS_CODE, O.PROTECT, O.REACT, O.RECOVERY, OE.AVAILABILITY_OF_SERVICE, and OE.MISUSE_DETECTION

FPT_PHP.2 Notification of Physical Attack
This component applies to the Access Control and Security Administration categories. The TOE must detect attempts to physically tamper with TOE security features, especially attempts to tamper with cryptographic components, Cross-Domain security systems, and systems listed in the Security Target. After detecting physical tampering, the TOE will notify TOE administrators.
Objectives addressed: O.ERROR_REJECT, O.PROTECT, O.PROTECT_EXT_COMMS, O.REACT, OE.ACCESS_PHYSICAL, OE.DISTRIBUTION, and OE.MISUSE_DETECTION

FPT_RCV.2 Automated Recovery
This component applies to the Access Control, Cross-Domain, and Security Administration categories. The TOE must be designed to automatically recover from events such as loss of electrical power or network connectivity without degradation of TOE security. If the TOE is unable to recover, then the TOE must enter a secure state. The Security Target may specify additional events or discontinuities from which the TOE must automatically recover.
Objectives addressed: O.ERROR_REJECT, O.PROTECT, O.PROTECT_EXT_COMMS, O.REACT, O.RECOVERY, O.TOE_FAILSAFE, OE.AVAILABILITY_OF_SERVICE, and OE.MISUSE_DETECTION

FPT_RPL.1 Replay Detection
This component applies to the Access Control category so that the TOE is able to detect attempts to masquerade as a TOE administrator by replaying the administrator's login and authentication entries. TOE Security Administrators can configure the TOE to also detect replay attempts against specified TOE user accounts.
Objectives addressed: O.AUTHORIZED_USE, O.ERROR_REJECT, O.NON-REPUDIATION, O.PROTECT, O.REACT, OE.MISUSE_DETECTION, OE.PROTECT_SECRETS, and OE.SPLIT_ADMIN

FPT_RVM.1 Non-Bypassability of the TSP
This component applies to the Access Control and Cross-Domain Filtering categories. The TOE security policy enforcement functions must always be invoked and properly functioning.
Objectives addressed: O.AUTHENTICATION, O.AUTHORIZED_USE, and O.PROTECT

FPT_SEP.3 Complete Reference Monitor
This component applies to the Security Admin and Cross-Domain Filtering categories. The TSF must protect itself against tampering that might compromise its security functionality. Additionally, the separation of TOE administration roles requires separation of the TSF from the rest of the TOE.
Objectives addressed: O.AUTHORIZED_USE, O.ERROR_REJECT, O.PROHIBIT_MALICIOUS_CODE, OE.PROTECT_SECRETS, OE.SPLIT_ADMIN, OE.SPLIT_ADMIN_SECURITY, and OE.SPLIT_ADMIN_SYSTEM

FPT_STM.1 Reliable Time Stamps
This component applies to all categories. Reliable time stamps are necessary for proper audit recording and analysis, some access controls, and for other TOE security functions.
Objectives addressed: O.AUDIT, O.NON-REPUDIATION, OE.BACKUP, and OE.DUE_CARE

FPT_TDC.1 Inter-TSF Basic Data Consistency
This component applies to the Access Control and Cross-Domain Filtering categories. The TOE must be able to consistently interpret access control data and Cross-Domain security enforcement attributes so that no individual, group, Community of Interest, or team of partner personnel is able to violate TOE security policies or partner security policies.
Objectives addressed: O.AUTHORIZED_USE, O.ERROR_REJECT, O.PROTECT, and OE.MISUSE_DETECTION

FPT_TST.1 TSF Testing
This component applies to the Access Control, Cross-Domain, and Security Administration categories. The TOE security functionality must pass a suite of self-tests prior to operation. Also, the TOE must periodically perform the suite of tests during operation and when activated by TOE administrators. The Security Target may specify additional conditions for when the suite of TSF self-tests is to be performed.
Objectives addressed: O.MANAGE, O.PROHIBIT_MALICIOUS_CODE, O.PROTECT, OE.DUE_CARE and OE.MISUSE_DETECTION

6.3.9 Class FRU: Resource Utilization

FRU_FLT.1 Degraded Fault Tolerance
This component applies to the Cross-Domain and Security Administration categories. As a fallback position to FPT_RCV.2 Automated Recovery, the TOE must go into a fail-safe condition when the TOE is unable to automatically recover from a failure that the TOE had been designed to handle. When automatic recovery to secure operation is not possible, the TOE will save all data and TSF files prior to entering the fail-safe condition.

Objectives addressed: O.PROTECT, O.REACT, O.TOE_FAILSAFE, OE.AVAILABILITY_OF_SERVICE, and OE.MISUSE_DETECTION

FRU_RSA.1 Maximum Quotas

This component applies to the Cross-Domain category. To limit the unauthorized disclosure rate that can result from a malicious user or administrator (known as an "insider attack"), TOE Cross-Domain security mechanisms must enforce an upper limit in the throughput rate for each authorized person's use of Cross-Domain transfers.

Objectives addressed: O.AUTHORIZED_USE, O.CROSS_DOMAIN_FILTERING, O.MANAGE, O.PROTECT, and OE.MISUSE_DETECTION

6.3.10 Class FTA: TOE Access

FTA_MCS.1 Basic Limitation on Multiple Concurrent Sessions

This component applies to the Access Control category. TOE System Administrators can set a maximum limit for concurrent sessions for all TOE users and administrators. This will reduce the likelihood of another person misusing an unattended session, which is important to reduce unauthorized access to COI information and administrator functions.

Objectives addressed: O.AUTHENTICATION, O.AUTHORIZED_USE, O.NON-REPUDIATION, and OE.PROTECT_SECRETS

FTA_MCS.2 Per User Limitation on Multiple Concurrent Sessions

This component applies to the Security Administration category and is necessary to ensure that a TOE Security Administrator cannot simultaneously login as a TOE System Administrator, and vice versa. This will help enforce the split administration policy for the TOE.

Objectives addressed: O.AUTHORIZED_USE, OE.GOOD_ADMIN, OE.SPLIT_ADMIN, OE.SPLIT_ADMIN_SECURITY, and OE.SPLIT_ADMIN_SYSTEM

FTA_SSL.1 TSF-Initiated Session Locking

This component applies to the Access Control and Security Administration categories. This component is necessary to minimize the amount of time that an unattended terminal session remains active. This helps reduce the risk of an insider attack, perhaps to gain access to COI information or to hide malicious activity behind another user's identity.

Objectives addressed: O.AUTHENTICATION, O.AUTHORIZED_USE, O.NON-REPUDIATION, O.PROTECT, and O.TOE_FAILSAFE

FTA_SSL.2 User-Initiated Session Locking

This component applies to the Access Control and Security Administration categories and allows each user and administrator to lock an interactive terminal session and then leave the terminal for a short period of time. This reduces the likelihood of another user or administrator misusing the terminal session, perhaps to gain access to COI information or to hide malicious activity behind the first user's identity.

Objectives addressed: O.AUTHENTICATION, O.AUTHORIZED_USE, O.NON-REPUDIATION, O.PROTECT, and O.TOE_FAILSAFE

FTA_SSL.3 TSF-Initiated Termination
This component applies to the Access Control category. The TOE must terminate unattended interactive terminal sessions, even if locked by the TSF or by the user, when the duration of the unattended session reaches a threshold set by the TOE Security Administrator. This ensures that no active terminal sessions remain undetected, possibly providing an opportunity for malicious insider activity.
Objectives addressed: O.PROTECT, O.TOE_FAILSAFE, and OE.AVAILABILITY_OF_SERVICE

FTA_TAB.1 Default TOE Access Banners
This component applies to the Security Administration category. U.S. federal and defense policies mandate the use of access banners. TOE Security Administrators need to be able to modify the access banners because the text of the banner may have to change, depending on the multinational membership and other factors.
Objectives addressed: O.MANAGE and OE.DUE_CARE

FTA_TAH.1 TOE Access History
This component applies to the Access Control category. In a multinational environment, the TOE must detect unauthorized access to each TOE login account as early as possible. Informing each user and administrator of recent login failures and successes helps to detect unauthorized access attempts.
Objectives addressed: O.AUTHORIZED_USE, O.PROTECT, OE.DUE_CARE, and OE.MISUSE_DETECTION

FTA_TSE.1 TOE Session Establishment
This component applies to the Access Control category. The mandatory access control policy requires the TOE to deny access to the TOE if the user cannot provide valid identity and authentication information.
Objectives addressed: O.AUTHENTICATION, O.AUTHORIZED_USE, O.NON-REPUDIATION, O.PROTECT, O.TOE_FAILSAFE, and OE.MISUSE_DETECTION

6.3.11 Class FTP: Trusted Path/Channels

FTP_ITC.1 Inter-TSF Trusted Channel
This component applies to the Security Administration category and is used to maintain confidentiality and integrity of audit data during transmission between the TOE and the TSE. Additional data types also will be transferred via a secured or trusted communication channel as described in the Security Target.
Objectives addressed: O.AUTHORIZED_USE, O.PROTECT, and OE.DUE_CARE

FTP_TRP.1 Trusted Path
This component applies to the Cross-Domain Filtering and Transmission Security categories. To ensure that TOE users do not accidentally gain access to TOE administrator functions, TOE

administrator authentication must be via a secured or trusted communication path. This also helps protect administrator identification and authentication information from being disclosed. Objectives addressed: O.AUTHENTICATION, O.AUTHORIZED_USE, O.MANAGE, O.PROTECT, OE.DUE_CARE, and OE.PROTECT_SECRETS

6.4 Security Assurance Requirements Rationale

As presented in Section 2.3, the TOE security functions have been grouped into four categories: Access control, Cross-Domain Filtering, Security Administration, and Transmission Security. As explained in Section 5.2.4, this PP defers Transmission Security requirements to the NSA Information Assurance Directorate because of the need for high assurance mechanisms (such as Type 1 cryptography) to protect classified information being transmitted between information domains.

The assurance level is EAL 5 Augmented for the Cross-Domain Filtering security category and EAL 4 Augmented for the Access control and Security Administration categories. This combination of assurance levels provides a high level of confidence in the security functions used to protect classified information in an MNIS environment. This assurance selection is based on these factors:

- The data flow analysis detailed in Section 2.2.3;
- Policy and threat considerations detailed in Chapter 3;
- EAL requirements specified in the Common Criteria Part 3, Annex B, "Cross reference of EALs and assurance requirements"; and
- Guidance provided in the Information Assurance Technical Framework document[39] regarding robustness issues (see also Section 6.6.2).

6.4.1 EAL Rationale

The following two subsections provide the rationale for EAL 5 Augmented for the Cross-Domain Filtering category of functionality and for EAL 4 Augmented for the Access Control and Security Administration categories. The rationale for each of the augmented assurance components follows in Subsection 6.4.2. Table 9 reiterates all of the assurance components for the MNIS TOE and identifies which of the assurance components are associated with each of the three categories of security functionality (excluding Transmission Security).

Table 9 - Summary of MNIS TOE Assurance Components

Assurance class	EAL 4 Components	EAL 5 Components	EAL 6 Components
Class ACM: Configuration	ACM_AUT.1 Partial CM automation *(AC and SA)*		ACM_AUT.2 Complete CM automation *(CD)*

[39] *Information Assurance Technical Framework*, Release 3, Section 4.5.2, National Security Agency, September 2000. See also http://www.iatf.net/.

Assurance class	EAL 4 Components	EAL 5 Components	EAL 6 Components
management	ACM_CAP.4 Generation support and acceptance procedures		
	ACM_SCP.2 Problem tracking CM coverage *(AC and SA)*	ACM_SCP.3 Development tools CM coverage *(CD)*	
Class ADO: Delivery and operation	ADO_DEL.2 Detection of modification		
	ADO_IGS.1 Installation, generation, and start-up procedures		
Class ADV: Development	ADV_FSP.2 Fully defined external interfaces *(AC and SA)*	ADV_FSP.3 Semiformal functional specification *(CD)*	
		ADV_HLD.3 Semiformal high-level design	
		ADV_IMP.2 Implementation of the TSF	
		ADV_INT.1 Modularity	
			ADV_LLD.2 Semiformal low-level design
		ADV_RCR.2 Semiformal correspondence demonstration	
	ADV_SPM.2 Semiformal TOE security policy model *(AC and SA)*	ADV_SPM.3 Formal TOE security policy model *(CD)*	
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance		
	AGD_USR.1 User guidance		
Class ALC: Life cycle support	ALC_DVS.1 Identification of security measures		
	ALC_FLR.3 Systematic flaw remediation		
	ALC_LCD.1 Developer defined life-cycle model *(AC and SA)*	ALC_LCD.2 Standardized life-cycle model *(CD)*	
	ALC_TAT.1 Subset of the implementation of the TSF *(AC and SA)*	ALC_TAT.2 Compliance with implementation standards *(CD)*	
Class ATE: Tests	ATE_COV.2 Analysis of coverage *(AC)*		ATE_COV.3 Rigorous analysis of coverage *(CD and SA)*
		ATE_DPT.2 Testing: low-level design	
			ATE_FUN.2 Ordered functional testing
	ATE_IND.2 Independent testing--sample		
Class AVA: Vulnerability assessment		AVA_CCA.1 Covert channel analysis *(CD)*	
	AVA_MSU.2 Validation of analysis *(AC and SA)*		AVA_MSU.3 Analysis and testing for insecure states *(CD)*
	AVA_SOF.1 Strength of TOE security function evaluation		
		AVA_VLA.3 Moderately resistant	

6.4.1.1 Rationale for EAL 5 Augmented

Table B.1[40] in the Common Criteria, Part 3 indicates that EAL 6 is the lowest EAL that incorporates the entire range of assurance components for the Cross-Domain Filtering category. This is because assurance components such as ACM_AUT.2 (Complete CM automation), ADV_LLD.2 (Semiformal low-level design), ATE_COV.3 (Rigorous analysis of coverage), ATE_FUN.2 (Ordered functional testing), and AVA_MSU.3 (Analysis and testing of insecure

[40] *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements*, Version 2.1, Annex B, page 207, August 1999.

states) occur at EAL 6. However, some of the assurance components associated with EAL 6 are not necessary for the Cross-Domain Filtering category. Because subtracting constituent assurance components from an EAL is not part[41] of the Common Criteria standard, a lower EAL must be selected and then augmented with the higher assurance components. The targeted EAL for the Cross-Domain Filtering category is therefore EAL 5 Augmented. This minimum level of assurance is appropriate for the security function category that validates the flow of information into or out of the TOE. The rationale for the Cross-Domain Filtering components that are augmented to EAL 6 is provided in Subsection 6.4.2 (below).

6.4.1.2 Rationale for EAL 4 Augmented

Similarly, Table B.1 in the Common Criteria, Part 3 indicates that EAL 6 is the lowest EAL that incorporates the entire range of assurance components for the Access Control and Security Administration categories. For example, assurance components ADV_LLD.2 (Semiformal low-level design) and ATE_FUN.2 (Ordered functional testing) are required for each category. As before, not all of the assurance components associated with EAL 6 are necessary for these two categories. However, EAL 5 Augmented is not appropriate for these categories because ACM_SCP.3 (Development tools CM coverage) and not ACM_SCP.2 (Problem tracking CM coverage) would be required. Additionally, most of the assurance components for these two categories are at the EAL 4 level and not the EAL 5 level. Therefore, the targeted EAL for the Access Control and Security Administration categories is EAL 4 Augmented. The rationale for the Access Control and Security Administration components that are augmented to EAL 5 or EAL 6 is provided in Subsection 6.4.2 (below).

6.4.2 Rationale for Augmented Assurance Components

The following subsections provide the rationale for each augmented component.

6.4.2.1 Rationale for ACM_AUT.2

ACM_AUT.2 (an EAL 6 requirement) is necessary to augment the Cross-Domain Filtering category because this category is critical in ensuring only authorized information flows into and out of the TOE. Therefore, "complete configuration management automation" must be present to track and control changes to the mechanisms comprising this category. ACM_AUT.1 (EAL 4 and 5) is sufficient for the other two categories because they operate within the physically and cryptographically protected TOE.

6.4.2.2 Rationale for ADV_FSP.3

ADV_FSP.3 (an EAL 5 requirement) is necessary for the Cross-Domain Filtering category because a semiformal functional specification helps assure that TOE's security functional requirements have been identified and specified in the cross-domain boundary protection mechanisms. The other two categories require ADV_FSP.2 (EAL 4) because they operate

[41] *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements*, Version 2.1, paragraph 6.1, August 1999.

within the physically and cryptographically protected TOE and such detailed specification is not necessary.

6.4.2.3 Rationale for ADV_HLD.3

ADV_HLD.3 (an EAL 5 requirement) is assigned to all three functional categories. It is an augmented requirement for Access Control and Security Administration because a semiformal high-level design is a more complete presentation of the interfaces to the many subsystems involved. Such detail will enable better and more appropriate testing of security functionality than is provided via ADV_HLD.2.

6.4.2.4 Rationale for ADV_IMP.2

ADV_IMP.2 (an EAL 5 requirement) is assigned to all three functional categories. It is an augmented requirement for Access Control and Security Administration because of the importance of determining an accurate and complete implementation of the TOE security functional requirements.

6.4.2.5 Rationale for ADV_INT.1

ADV_INT.1 (an EAL 5 requirement) is assigned to all three functional categories. It is an augmented requirement for Access Control and Security Administration because modularity will help with developing, evaluating, and upgrading the TSF.

6.4.2.6 Rationale for ADV_LLD.2

ADV_LLD.2 (an EAL 6 requirement) augments all three functional categories because of the need for a low-level design of the TSF modules, which in turn will provide an accurate description of the internal workings of these modules and their interrelationships and dependencies. This component introduces the requirement for a complete presentation for the interfaces to the modules, which will provide necessary detail for supporting thorough testing and vulnerability assessment. ADV_LLD.1 (EAL 4 and 5) does not provide complete details for all interface effects.

6.4.2.7 Rationale for ADV_RCR.2

ADV_RCR.2 (an EAL 5 requirement) is assigned to all three functional categories. It is an augmented requirement for Access Control and Security Administration because of the need for level correspondence of the various TSF representations. Because semiformal representation is required in most of the TSF representations, it is reasonable to require that the correspondence between the representations be semiformal rather than informal (ADV_RCR.1).

6.4.2.8 Rationale for ATE_COV.3

ATE_COV.3 (an EAL 6 requirement) augments the Cross-Domain Filtering and Security Administration categories because of the need for rigorous analysis of test coverage for these two categories. The split administration requirement is vital to the security of the MNIS TOE and,

therefore, rigorous testing is required. Likewise, rigorous testing is also required for high assurance cross-domain filtering functions. On the other hand, ATE_COV.2 analysis of coverage (EAL 3-5) is appropriate for the category of Access Control functionality within the TOE because of the security provided in a physically and cryptographically protected environment.

6.4.2.9 Rationale for ATE_DPT.2

ATE_DPT.2 (an EAL 5 requirement) is assigned to all three functional categories. It is an augmented requirement for Access Control and Security Administration to test in detail security functions described by the low-level design of the TOE. Thus, the security functions described in both low and high-level designs are tested.

6.4.2.10 Rationale for ATE_FUN.2

ATE_FUN.2 (an EAL 6 requirement) augments all three functional categories to demonstrate that all security functions perform as specified. The developer must perform tests and provide test documentation. All testing must be structured to avoid circular arguments regarding functional correctness. The structured nature of this requirement is what is required in this EAL 6 requirement for the security subsystems of the MNIS system.

6.4.2.11 Rationale for AVA_CCA.1

AVA_CCA.1 (an EAL 5 requirement) is necessary for the Cross-Domain Filtering category to ensure that a covert channel analysis has been performed on the mechanisms that interconnect the TOE to the external domains. Such analysis is not needed for the other two categories because they operate strictly within the physically and cryptographically protected MNIS information domain.

6.4.2.12 Rationale for AVA_MSU.3

AVA_MSU.3 (an EAL 6 requirement) is necessary to augment the Cross-Domain Filtering category because cross-domain functions validate and transfer communications between the MNIS TOE and other information domains. This requirement ensures that misleading, unreasonable, and conflicting guidance is absent from guidance documentation. Also, this requirement ensures that secure procedures for all modes of operation of the subsystems of this category have been addressed. The evaluator is required to perform independent testing to determine that an administrator or user, with an understanding of the guidance documentation, would reasonably determine if the Cross-Domain Filtering system is configured and operating in an insecure manner. AVA_MSU.2 (EAL 4 and 5) is sufficient for the other two categories because they operate strictly within the physically and cryptographically protected MNIS information domain and such detailed vulnerability assessment is not necessary.

6.4.2.13 Rationale for AVA_VLA.3

AVA_VLA.3 (an EAL 5 requirement) is assigned to all three functional categories. It is an augmented requirement for Access Control and Security Administration to ensure that proper

vulnerability assessments have been accomplished. This component requires that a systematic search for vulnerabilities be performed, assuring that the functions provided are more resistant to a potential attack.

6.5 Dependencies Mapping

When using the Common Criteria, dependencies exist when one component is not self-sufficient and relies upon the presence of another component. The following two sections list the dependencies among the TOE requirements. The dependencies that result from the functional requirements are in Section 6.5.1 and the dependencies from the assurance requirements are in Section 6.5.2. Proper TOE function is also dependent on external entities. Section 6.5.3 describes in general terms the nature of the dependencies between the TOE and external entities.

6.5.1 Satisfaction of Functional Requirements Dependencies

The following table lists all of the dependencies that result from the TOE security functional requirements. A comparison of the requirements listed in the second column of the table with the requirements listed in Chapter 5 indicates that all of the dependencies have been met.

Table 10 - Functional Requirement Dependencies

Functional Requirement	Requirements Depended On
FAU_ARP.1 Security Alarms	FAU_SAA.1 Potential violation analysis
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps
FAU_GEN.2 User identity association	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification
FAU_SAA.1 Potential violation analysis	FAU_GEN.1 Audit data generation
FAU_SAA.2 Profile based anomaly detection	FIA_UID.1 Timing of identification
FAU_SAR.1 Audit review	FAU_GEN.1 Audit data generation
FAU_SAR.2 Restricted audit review	FAU_SAR.1 Audit review
FAU_SAR.3 Selectable audit review	FAU_SAR.1 Audit review
FAU_SEL.1 Selective audit	FAU_GEN.1 Audit data generation FMT_MTD.1 Management of TSF data
FCO_NRO.1 Selective proof of origin	FIA_UID.1 Timing of identification
FCS_CKM.1 Cryptographic key generation	FCS_CKM.2 Cryptographic key distribution FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes
FCS_CKM.2 Cryptographic key distribution	FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes
FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 Cryptographic key generation FMT_MSA.2 Secure security attributes

Functional Requirement	Requirements Depended On
FCS_COP.1 Cryptographic operation	FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes
FDP_ACC.2 Complete access control	FDP_ACF.1 Security attribute based access control
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ETC.2 Export of user data with security attributes	FDP_ACC.1 Subset access control[42]
FDP_IFC.1 Subset information flow control (for the access control category)	FDP_IFF.1 Simple security attributes
FDP_IFC.2 Complete information flow control (for the cross-domain filtering and security administration categories)	FDP_IFF.1 Simple security attributes
FDP_IFF.1 Simple security attributes	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization
FDP_IFF.2 Hierarchical security attributes	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization
FDP_IFF.3 Limited illicit information flows	AVA_CCA.1 Covert channel analysis FDP_IFC.1 Subset information flow control
FDP_ITC.2 Import of user data with security attributes	FDP_ACC.1 Subset access control[43] FTP_TRP.1 Trusted path FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITT.2 Transmission separation by attribute	FDP_ACC.1 Subset access control *or* FDP_IFC.1 Subset information flow control (only for the access control category)
FDP_ROL.1 Basic rollback	FDP_ACC.1 Subset access control[44]
FIA_AFL.1 Authentication failure handling	FIA_UAU.1 Timing of authentication
FIA_UAU.2 User authentication before any action	FIA_UID.1 Timing of identification
FIA_UAU.7 Protected authentication feedback	FIA_UAU.1 Timing of authentication
FIA_USB.1 User-subject binding	FIA_ATD.1 User attribute definition
FMT_MOF.1 Management of security functions behavior	FMT_SMR.1 Security roles

[42] Note: Part 2 of the CC indicates that FDP_ETC.2 has a dependency on either FDP_ACC.1 or FDP_IFC.1. However, FDP_ETC.2 is a requirement for the cross-domain filtering category and FDP_IFC.1 does not apply to that category.

[43] Note: Part 2 of the CC indicates that FDP_ITC.2 has a dependency on either FDP_ACC.1 or FDP_IFC.1. However, FDP_ITC.2 is a requirement for the cross-domain filtering category and FDP_IFC.1 does not apply to that category.

[44] Note: Part 2 of the CC indicates that FDP_ROL.1 has a dependency on either FDP_ACC.1 or FDP_IFC.1. However, FDP_ROL.1 is a requirement for the security administration category and FDP_IFC.1 does not apply to that category.

Functional Requirement	Requirements Depended On
FMT_MSA.1 Management of security attributes	FDP_ACC.1 Subset access control *or* FDP_IFC.1 Subset information flow control (only for the access control category) FMT_SMR.1 Security roles
FMT_MSA.2 Secure security attributes	ADV_SPM.1 Informal TOE security policy model FDP_ACC.1 Subset access control *or* FDP_IFC.1 Subset information flow control (only for the access control category) FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3 Static attribute initialization	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MTD.1 Management of TSF data	FMT_SMR.1 Security roles
FMT_MTD.2 Management of limits on TSF data	FMT_MTD.1 Management of TSF data FMT_SMR.1 Security roles
FMT_MTD.3 Secure TSF data	ADV_SPM.1 Informal TOE security policy model FMT_MTD.1 Management of TSF data
FMT_REV.1 Revocation	FMT_SMR.1 Security roles
FMT_SMR.1 Security roles	FIA_UID.1 Timing of identification
FMT_SMR.2 Restrictions on security roles	FIA_UID.1 Timing of identification
FMT_SMR.3 Assuming roles	FMT_SMR.1 Security roles
FPT_FLS.1 Failure with Preservation of Secure State	ADV_SPM.1 Informal TOE security policy model
FPT_ITT.3 TSF data integrity monitoring	FPT_ITT.1 Basic internal TSF data transfer protection
FPT_PHP.2 Notification of physical attack	FMT_MOF.1 Management of security functions behavior
FPT_RCV.2 Automated Recovery	FPT_TST.1 TSF testing ADV_SPM.1 Informal TOE Security Policy Model AGD_ADM.1 Administrator Guidance
FPT_TST.1 TSF testing	FPT_AMT.1 Abstract machine testing
FRU_FLT.1 Degraded fault tolerance	FPT_FLS.1 Failure with preservation of secure state
FTA_MCS.1 Basic limitation on multiple concurrent sessions	FIA_UID.1 Timing of identification
FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions	FIA_UID.1 Timing of identification
FTA_SSL.1 TSF-initiated session locking	FIA_UAU.1 Timing of authentication
FTA_SSL.2 User-initiated session locking	FIA_UAU.1 Timing of authentication

6.5.2 Satisfaction of Assurance Requirement Dependencies

The following table lists all of the dependencies that result from the TOE security assurance requirements. A comparison of the requirements listed in the second column of the table with the requirements listed in Section 5.3 indicates that all of the dependencies have been met.

Table 11 - Assurance Requirements Dependencies

Assurance Requirement	Requirements Depended On
ACM_AUT.2 Complete CM automation	ACM_CAP.3 Authorization controls
ACM_CAP.4 Generation Support and Acceptance Procedures	ACM_SCP.1 TOE CM coverage ALC_DVS.1 Identification of security measures
ACM_SCP.3 Developmental tools CM coverage	ACM_CAP.3 Authorization controls
ADO_DEL.2 Detection of modification	ACM_CAP.3 Authorization controls
ADO_IGS.1 Installation, generation, and start-up procedures	AGD_ADM.1 Administrator guidance
ADV_FSP.3 Semiformal functional specification	ADV_RCR.1 Informal correspondence demonstration
ADV_HLD.3 Semiformal high-level design	ADV_FSP.3 Semiformal functional specification ADV_RCR.2 Semiformal correspondence demonstration
ADV_IMP.2 Implementation of the TSF	ADV_LLD.1 Descriptive low-level design ADV_RCR.1 Informal correspondence demonstration ALC_TAT.1 Well-defined development tools
ADV_INT.1 Modularity	ADV_IMP.1 Subset of the implementation of the TSF ADV_LLD.1 Descriptive low-level design
ADV_LLD.2 Semiformal low-level design	ADV_HLD.3 Semiformal high-level design ADV_RCR.2 Semiformal correspondence demonstration
ADV_SPM.3 Formal TOE security policy model	ADV_FSP.1 Informal Functional specification
AGD_ADM.1 Administrator guidance	ADV_FSP.1 Informal Functional specification
AGD_USR.1 User guidance	ADV_FSP.1 Informal Functional specification
ALC_TAT.2 Compliance with implementation standards	ADV_IMP.1 Subset of the implementation of the TSF
ATE_COV.3 Rigorous Analysis of Coverage	ADV_FSP.1 Informal functional specification ATE_FUN.1 Functional testing
ATE_DPT.2 Testing: low-level design	ADV_HLD.2 Security enforcing high-level design ADV_LLD.1 Descriptive low-level design ATE_FUN.1 Functional testing
ATE_IND.2 Independent Testing--Sample	ADV_FSP.1 Informal functional specification AGD_ADM.1 Administrator guidance AGD_USR.1 User guidance ATE_FUN.1 Functional testing

Assurance Requirement	Requirements Depended On
AVA_CCA.1 Covert channel analysis	ADV_FSP.2 Fully defined external interfaces ADV_IMP.2 Implementation of the TSF AGD_ADM.1 Administrator guidance AGD_USR.1 User guidance
AVA_MSU.3 Analysis and Testing for Insecure States	ADO_IGS.1 Installation, generation, and start-up procedures ADV_FSP.1 Informal functional specification AGD_ADM.1 Administrator guidance AGD_USR.1 User guidance
AVA_SOF.1 Strength of TOE security function evaluation	ADV_FSP.1 Informal functional specification ADV_HLD.1 Descriptive high-level design
AVA_VLA.3 Moderately Resistant	ADV_FSP.1 Informal functional specification ADV_HLD.2 Security enforcing high-level design ADV_IMP.1 Subset of the implementation of the TSF ADV_LLD.1 Descriptive low-level design AGD_ADM.1 Administrator guidance AGD_USR.1 User guidance

6.5.3 TOE Dependencies on External Entities

The security of the TOE depends not only on the functionality within the TOE, but also on functions that are performed outside of the TOE. For example, Section 4.2 identified security objectives for the TOE Security Environment (TSE). Furthermore, the cross-domain filtering requirements described in Section 5.2.2 levy requirements on U.S. and partner IT systems that are not part of the TOE or the TSE. Specifically, the U.S. and its partners have to comply with MNIS cross-domain policies and procedures to be allowed to transfer information into the MNIS Environment. As a result, TOE developers and implementers must not only implement and integrate security functions across the TOE and the TSE, but they also must coordinate with the security administrators and system operators of the external U.S. and partner systems that will interact with the TOE.

6.6 Robustness and Strength of Mechanism Rationale

The rationale for the TOE's security robustness or Strength of Mechanism Level (SML) is based on the threat potential identified in this Protection Profile. Two strengths of robustness are appropriate for the MNIS TOE. This is because the MNIS TOE has two separate threat levels, one for the external threat to the TOE and the other for the threat from multinational users within the MNIS Environment (see also A.THREAT_LEVEL in Section 3.3.) Additionally, the MNIS PP, unlike most protection profiles, describes a TOE that consists of a system of systems and not a single component or subsystem.

More than one method exists to select the appropriate robustness or SML level for an IT system.[45] Each of the following two subsections applies a different method. In each case, the method is applied to both the entire MNIS TOE (external threat to the TOE) and to the internal TOE threat from authorized users.

6.6.1 DOD CIO Guidance and Policy Memorandum 6-8510

Applying the guidance in DoD Chief Information Officer Guidance and Policy Memorandum Number 6-8510, "Department of Defense Global Information Grid Information Assurance" (16 June 2000), the robustness level for the entire MNIS TOE is HIGH. This level of robustness is necessary for external access to the TOE associated with transmission security, cross-domain filtering, and access control. However, within the MNIS TOE, lower robustness is appropriate, typically equivalent to commercial cryptographic, security administration, and access control systems that can operate at a MEDIUM robustness level. For example, MEDIUM robustness services can be used to control access to Community of Interest (COI) information within the MNIS TOE.

6.6.2 Information Assurance Technical Framework

Applying the guidance in the "Determining the Degree of Robustness" section[46] of the *Information Assurance Technical Framework* provides a more detailed perspective on security robustness of the MNIS Environment. Combining each of the two TOE threat levels with the TOE information value[47] generates two pairs of strength of mechanism level (SML) and evaluated assurance level (EAL) numbers. The combination of TOE information value V4 with the threat level of T5 from outside the TOE results in SML3/EAL5. Similarly, the combination of the information value V4 with the threat level of T2 within the MNIS TOE results in SML2/EAL2. The following paragraphs discuss these results with respect to the four categories of TOE security functionality.

6.6.2.1 High Robustness

High robustness (SML3/EAL5) is necessary to protect the TOE from external threats. This level directly applies to the functional security categories of transmission control and cross-domain filtering. For example, NSA-approved (Type 1) cryptography is required to protect the transmission of classified information between protected MNIS facilities. Similarly, high assurance guarding systems are necessary to validate the transfer of all information across the MNIS Information Domain boundary and to block the transfer of malicious content. EAL 5 is the minimum assurance level and, in the case of cross-domain filtering, certain assurance components are augmented above EAL 5 as described in Section 6.4.

---

[45] Various guidance documents define security strength in terms of "robustness of mechanisms," "robustness levels," "strength of function," or "strength of mechanism level". This PP uses these terms interchangeably unless referring to a title in a particular publication.

[46] "*Information Assurance Technical Framework*", Release 3, Section 4.5.2, National Security Agency, September 2000. See also http://www.iatf.net/.

[47] See also A.INFORMATION_VALUE and A.THREAT_LEVEL in Section 3.3, "TOE Assumptions".

6.6.2.2 Medium Robustness

Medium robustness (SML2/EAL2) applies only to the "shoulder-to-shoulder" working environment within the MNIS Information Domain. However, this level of robustness is not sufficient for protecting the classified information processed by the MNIS TOE. The TOE users and administrators are from multiple nations and they are supporting multinational military operations. Therefore, additional security functionality and assurance are required above the EAL 2 level. For example, individual attribution and auditing of all user activities requires a higher robustness for Access Control. Similarly, the multinational TOE membership increases the security functionality and assurance associated with Security Administration. As a result, EAL 4 Augmented is the minimum level for the access control and security administration categories. Section 6.4 explains which assurance components are augmented for these two categories.

Appendix A - Acronyms

ASCII	American Standard Code for Information Interchange
CC	Common Criteria
CIP	Common Intelligence Picture
COE	Defense Information Infrastructure Common Operating Environment
COI	Community of Interest
COP	Common Operational Picture
C/S/A	Combatant Command, Service, or Agency
DIA	Defense Intelligence Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
EAL	Evaluation Assurance Level
FDO	Foreign Disclosure Officer
HTML	Hypertext Markup Language
I&A	Identification and Authentication
IT	Information Technology
LAN	Local Area Network
MNIS	Multinational Information Sharing
MNIS PP	MNIS Protection Profile
ORD	Operational Requirements Document
PP	Protection Profile
RBAC	Role-Based Access Control
SF	Security Function
SFP	Security Function Policy
SIPRNET	Secret Internet Protocol Router Network
SOF	Strength of Function
SOO	Statement of Objectives
SSAA	System Security Accreditation Agreement
SSE	System Security Engineer
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSE	TOE Security Environment
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
UPC	Unique Planning Components
VPN	Virtual Private Network
WAN	Wide Area Network
XML	Extensible Markup Language

Appendix B - References

a. Common Criteria Implementation Board, *Common Criteria for Information technology Security Evaluation,* Part 1 Introduction and general model CCIB-99-031, Version 2.1, August 1999.
b. Common Criteria Implementation Board, *Common Criteria for Information technology Security Evaluation,* Part 2 Security Functional Requirements CCIB-99-032, Version 2.1, August 1999.
c. Common Criteria Implementation Board, *Common Criteria for Information technology Security Evaluation,* Part 3 Security Assurance Requirements CCIB-99-033, Version 2.1, August 1999.
d. Common Criteria Implementation Board, *Common Methodology for Information technology Security Evaluation,* Part 2 Evaluation Methodology CEM-99/045, Version 1.0, August 1999.
e. *National Information System Security (INFOSEC) Glossary*, NSTISSI No. 4009, January 1999 (Revision 1).
f. DoD Information Assurance Guidance and Policy Memorandum, 16 Jun 2000.
g. Director Central Intelligence Directive (DCID) 6/3, *Protecting Sensitive Compartmented Information within Information Systems*, 5 June 1999.
h. AFSSI 5027, *Network Security Policy*, 27 February 1998.
i. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No.11, "National Information Assurance Acquisition Policy", Jan 2000.
j. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 3006.
k. *Joint Vision 2020, U.S. Department of Defense*, June 2000 (http://www.dtic.mil/jv2020/)
l. *Information Assurance Technical Framework*, Release 3.0, National Security Agency, September 2000 (http://www.iatf.net/framework_docs/version-3_0/).
m. *DoD Information Technology Security Certification and Accreditation Process*, DoD Instruction 5200.40, 30 December 1997.

Appendix C - Glossary of Commonly Used Terms

Alliance - An alliance is the result of formal agreements (i.e., treaties) between two or more nations for broad, long-term objectives that further the common interests of the members. See also coalition. (Approved by JMTGM# 094-0556-94)

Allies - Assigned forces in a U.S. joint command. Forces and resources placed under the Combatant Command by the U.S. Secretary of Defense in his "Forces for Unified Command" memorandum and available for normal peacetime operations. (User's Guide for Joint Operation Planning)

Coalition - A force composed of military elements of nations that have formed a temporary alliance for some specific purpose. (JP 1-02)

Combined – A union of two or more forces, agencies, or more allies. (When all allies or services are not involved, the participating nations and services shall be identified, e.g., Combined Navies.) See also *joint*. (JP 1-02)

Command and Control - The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C^2 (Approved by JMTGM# 076-2864-94)

Community of Interest (COI) – A group of authorized users that may communicate with each other within the MNIS Information Domain using "need-to-know" data separation mechanisms. Note: Commercial mechanisms that provide medium robustness data separation are sufficient to provide "need-to-know" separation.

Highly-formatted data - Data that is very specific in content and format. This terminology may refer to measurement data, such as that data derived from a sensor and transmitted to a program that uses it to plot activity. Examples are radar data such as latitudes and longitudes and temperature data.

Information Domain - An information domain is defined as the virtual space in which all the contained information is classified at a ***single*** level and all personnel with physical or electronic access to that information are appropriately cleared and authorized to that level of information and resources.

Joint - Connotes activities, operations, organizations, etc., in which elements of two or more military departments participate. (Approved by JMTGM# 076-2864-94). NOTE: also connotes activities of two or more nations.

Joint Force or **Joint Task Force** - A general term applied to a force composed of significant elements, assigned or attached, of two or more military departments, operating under a single joint force commander. See also joint force commander. (Approved by JMTGM# 076-2864-94). NOTE: also connotes forces of two or more nations that may be of the same military department.

Joint Force Commander - A general term applied to a combatant commander, sub-unified commander, or joint task force commander authorized to exercise combatant command (command authority) or operational control over a joint force. See also *joint force*. (Approved by JMTGM# 076-2864-94)

Logistics - The science of planning and carrying out the movement and maintenance of forces. In its most comprehensive sense, those aspects of military operations that deal with: (a) design and development, acquisitions, storage, movement, distribution, maintenance, evacuation, and disposition of material; (b) movement, evacuation, and hospitalization of personnel; (c) acquisition or construction, maintenance, operation, and disposition of facilities; and (d) acquisition or furnishing of services. (Approved by JMTGM# 076-2864-94)

Material - All items (including ships, tanks, self-propelled weapons, aircraft, etc., and related spares, repair parts, and support equipment, but excluding real property, installation, and utilities) necessary to equip, operate, maintain, and support military activities without distinction as to its application for administrative or combat purposes. (JP 1-02)

Military Departments - One of the departments within the U.S. Department of Defense created by the U.S. National Security Act of 1947, as amended (Department of the Army, Navy, or Air Force). (JP 1-02)

Multinational - Multinational involves working with more than one nation.

Multinational Military Operations - Multinational military operation encompasses actions conducted by the combined forces of two or more nations in support of a common mission or objective.

Multinational Operations - Multinational operations encompasses actions conducted by more than one nation operating together in response to an international event(s) for the purpose of achieving a common mission or objective.

Multinational Partner - Includes allied military forces, coalition forces, alliances (such as NATO), government agencies, international organizations, and non-governmental organizations.

Partnership - Partnership is comprised of all nations that form the multinational operations.

Security Related Terminology

Accountability - An IS Property allowing auditing of IS activities to be traced to persons or processes that may then be held responsible for their actions. (NSTISSI 4009)

Agent - A Person, process, or agency.

Authenticity - The property that allows the ability to validate the claimed identity of a system entity. (DITSCAP)

Authorized Administrator - An Authorized user (e.g., Security Administrator (ISSO/ISSM), System Administrator, Database Administrator, Network Administrator, or Network Security Manager) who has been granted the authority to manage the TOE. These users are expected to use this authority only in the manner prescribed by the guidance given to them.

Authorized User - A user who has been properly identified and authenticated. These users are considered legitimate users of the TOE.

Availability - Timely, reliable access to data and information services for authorized users. (NSTISSI 4009/DITSCAP)

Component - The smallest selectable set of elements that may be included in a PP, an ST, or a package.

Confidentiality - Assurance that information is not disclosed to unauthorized persons, processes, or devices. (NSTISSI 4009/DITSCAP)

Controlled Information - Any information that is subject to security classification and need-to-know restrictions.

Controlled Object - Any system objects that are subject to security classification and need-to-know restrictions.

Controlled Subjects - Any system subjects that are subject to security classification and need-to-know restrictions.

Dependency - A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.

Element - Members of a component; cannot be selected individually.

Evaluation Assurance Level (EAL) - A package consisting of assurance components from CC, Part 3 that represents a point on the CC predefined assurance scale.

Host Identity - Identification of any systems with which the TOE communicates and which processes information from or supplies information to the TOE.

Information Security Attributes - Information component that should be maintained at the level of the user. Any additional attributes, other than the user's identity, that are used to enforce the TSP.

Integrity - The quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. In a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information. (NSTISSI 4009/DITSCAP)

Non-Repudiation - Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. (NSTISSI 4009)

Object - An entity within the TOE Security Functions Scope of Control (TSC) that contains or receives information and upon which subjects perform operations.

Package - A reusable set of either functional or assurance components (e.g., an EAL), combined together to satisfy a set of identified security objectives.

Periods Processing - Processing of various levels of classified and unclassified information at distinctly different times. Under the concept of periods processing, the system must be purged of all information from one processing period before transitioning to the next. (NSTISSI 4009)

Protection Profile (PP) - An implementation-independent set of security functional and assurance requirements for a category of TOEs that meet specific consumer needs.

Security Target (ST) - An implementation-specific set of security functional and assurance requirements and specifications to be used as the basis for evaluation of an identified TOE solution.

Secure Values - Additional characteristics deemed necessary for assigned security parameters, (e.g., passwords must include an upper case letter and at least one number or symbol).

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation (TOE) - An Information Technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions (TSF) - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP) - A set of rules that regulate how assets are managed, protected, and distributed within a TOE.

TSF Scope of Control (TSC) - The set of interactions that can occur with or within a TOE and are subject to the rules of the TOE security policy.

Unauthorized User - Any person that is not authorized under the TOE security policy to access the TOE.

User - Any person, process, or device that is authorized under the TOE security policy to access or interface with the TOE.

User Identity - A unique identification and name assigned to a user that when combined with a provided Password will be the basis for establishing authenticated user access to their account and the TOE.

Appendix D - MNIS Operational Scenarios

Scenario 1: Report Composition Utilizing Multiple Information Domain Sources

Users located within U.S.-Only, MNIS, and Partner National physical environments need the capability to access information from multiple information domains and multiple physical, distributed environments with the intent of composing reports for distribution to recipients with varying authorizations, who may be located in any physical environments. Reports may be generated for either a known set of recipients (in known environments) or, without pre-knowledge as to who the eventual recipients will be or where they are physically located.

Sources of Information:

- Local servers or other users located in the same information domain as the report author.
- Remote servers or other users located in information domains other than the report author's domain.
- Automatic feeds providing information directly to the report author's desktop.
- Sneaker Net input.
- Information stored on the local client workstation.

Characteristics of Report Information

- All reports have an author,
- Report information may be extracted from a labeled source that is classified the same as the desired classification of the report,
- Report information may be extracted from a labeled source that is classified hierarchically higher then the desired classification of the report. For example, the author extracts Secret information from a Top Secret source and includes it in a report that is to be classified Secret.
- Report information may be extracted from a labeled source that is classified hierarchically lower then the desired classification of the report. For example, the author includes in a Secret report information that is labeled UNCLASSIFIED and has been extracted from an UNCLASSIFIED source.

- Report information may be extracted from a labeled source that has been released to all desired recipients. For example, the author includes in an asserted US/REL A report information that has been extracted from a US/REL A & B source.
- Report information that is of indeterminate classification. For example, the author desires to include in a Secret report unlabeled information from a system-high source.

Desired Capability:

A report author desires the capability to access information that is locally stored on his or her own client, stored within their same physical environment, automatically pushed to the local client, and/or remotely stored in distant physical environments. The sources of information may contain information that is in the same information domain as the intended report or may be in a different information domain. Information from sources in a different information domain than the intended report will require re-grading or filtering before being added to the report.

To perform the report generation function it is desirable for the author to be able to establish sessions at multiple information domain levels on a single workstation (multiple windows at each authorization level displayed simultaneously). With these multiple information sources available, the user would then need to be able to selectively cut and paste information into a "report composition window." The report composition window would, by default, be established at the information domain level of the most restrictive session currently opened, but also be capable of indicting an "asserted" information domain level for the intended report, matching the authorization of the intended audience for the report.

For example, the report author would simultaneously open windows displaying information from Top Secret system-high sources, Secret system-high sources, and UNCLASSIFIED sources. The author would then open a composition window that, by default, would be established at a Top Secret level, but also **assert** that it will contain only UNCLASSIFIED information. The author would then be allowed to selectively cut information from all of these information sources and paste it into the report composition window. As information is pasted into the composition window, it would be labeled with it source classification level (e.g., Top Secret, Secret, and UNCLASSIFIED) and its asserted classification, UNCLASSIFIED.
After the author has completed the draft report, a person authorized to verify the classification or sensitivity level asserted by the author must approve the report. If the report is to be released to foreign nations, then a Foreign Disclosure Officer (FDO) must also concur that the report can be released in accordance with established policy.

Associated Security Services:

- Capability to maintain data separation, data integrity and data confidentiality of information contained within multiple information domains, simultaneously processed in, or stored on, a single client workstation.

- Capability to maintain data separation, data integrity and data confidentiality of information while it is transferred to/from a client's workstation.
- Capability to maintain binding of information to trusted data labels during data transfer, processing and storage.
- Capability to maintain binding of information to default, network, system-high data labels during data transfers processing and storage.
- Capability to bind an asserted data label to reports that are created on the client workstation, while it is being composed, stored on, or transferred to/from a person authorized to verify the classification or sensitivity level asserted by the author.
- Capability to perform "trusted cutting/pasting" operations between sessions that have been, established at differing information domain levels. By trusted cutting and pasting, the implication is that only selected information that is correctly displayed to the report author, is being pasted to the target composition window (e.g., no hidden code or deleted symbols are pasted, and "undo" operations are inhibited).
- Capability to perform filtering and virus testing of information that is extracted/cut from less privileged information domains prior to its pasting into a greater privileged information domain.
- Capability to perform sanitization filtering (e.g., dirty word searches) on information that is being extracted or transmitted from information domains of greater privilege into less privileged information domains.
- Capabilities to generate, maintain, transfer and properly associate, attribute and interpret relevant security related audit event records.
- Capability to receive, process, and transfer required security parameters to/from related security infrastructure components in support of authorized procedures and operations.
- Capability to reliably and unambiguously identify and authenticate users, administrators, and maintainers of the client workstation.
- Capability to reliably and correctly interpret and act upon the authorizations associated with identified and authenticated users, administrators and maintainers of client workstations.

Scenario 2: Report Distribution to Multiple Information Domains

Users located within U.S.-Only, MNIS, and Partner National physical environments need the capability to distribute reports to multiple information domains and physically dispersed environments destined for recipients having varying authorizations and who may be located in any physical environments.

Recipients/Destinations of the Reports:

- Local servers and clients located in the same physical environment as the distributing client.
- Remote servers and clients located in physical environments external to the distributing client's physical environment.
- Sneaker Net distribution channels.

Distributed Report Characteristics:

- A report may be distributed within its information domain,
- A report may be distributed to an information domain that contains information that is classified hierarchically higher than the classification of the report,
- A report may be distributed to recipients in different information domains after a review of its contents based on negotiated security policy and procedures.

Desired Capability:

A report author desires the capability to distribute information that is locally stored on his or her own client, to either destinations that are within, or external to, their same physical environment. The information may be distributed to recipients who are members of the same information domain or an information domain that is a hierarchical sub-set of the sending client's (e.g., U.S. Secret/REL. X & Y may be sent to U.S. Secret, U.S. Top Secret, Partner X Secret.) When the recipient is a member of an information domain that has authorization that is more restrictive then the sending client (e.g., recipient information domain is Secret, and sending client is a member of a Top Secret information domain), a re-grading or filtering operation is typically performed before the information is distributed and the report is reviewed by a person authorized to verify the classification or sensitivity level asserted by the author. In addition to re-grading/filtering and classification review, release of information to a recipient who is a member of a different information domain typically requires a releasability decision to be performed by a third party (e.g., Foreign Disclosure Officer review) prior to release.

To perform the report distribution function the client must be able to establish a session at the authorization level of both the information to be distributed and the intended recipient. If the distributing client workstation has the capability to generate, process and display information contained within multiple information domains (as described in the Report Composition Scenario) it is possible that multiple domain windows (all operating a different authorization levels) will be active simultaneously. In such a situation, the distributing client workstation must have the capability of supporting data separation/segregation requirements to insure that the distributed information is confined to the authorization level of the intended, authenticated recipient.

For example, the distributing client might simultaneously have open windows displaying information contained within a Top Secret system-high domain, a Secret domain, and an UNCLASSIFIED domain and want to distribute information that is U.S. Secret. Typically, the distributing client workstation negotiates a secure session with the destination workstation and releases information only from his established U.S. Secret window with appropriate security services. If third party review for classification and releasability is required prior to the release of information, it might be possible for the distributing client to open a distribution window which by default, would be established at a Top Secret level, but also **assert** that the formatted information exchange will contain only Secret information. After classification and releasability review, the information might then be actually released or, alternatively, returned to the distributing client for forwarding to the intended recipient.

Associated Security Services:

- Capability to maintain data separation, data integrity and data confidentiality of information contained within multiple information domains, simultaneously processed in, or stored on, a single client workstation.
- Capability to maintain data separation, data integrity and data confidentiality of information while it is be transferred to/from a client's workstation.
- Capability to maintain binding of information to trusted data labels during data transfer, processing and storage.
- Capability to maintain binding of information to default, network, system-high data labels during data transfers processing and storage.
- Capability to bind an asserted data label to reports that are created on the client workstation, while it is being composed, stored on, or transferred to/from a classification reviewer.
- Capability to perform re-grading and filtering of information prior to its distribution if it is originated on a client workstation that contains multiple information domains.
- Capabilities to generate, maintain, transfer and properly associate, attribute and interpret relevant security related audit event records.

- Capability to receive, process, and transfer required security parameters to/from related security infrastructure components in support of authorized procedures and operations.
- Capability to reliably and unambiguously identify and authenticate users, administrators, and maintainers of the client workstation.
- Capability to reliably and correctly interpret and act upon the authorizations associated with identified and authenticated users, administrators and maintainers of client workstations.

Scenario 3: Collaboration Among the US and its Partners

Users collaborate as they develop, assess, refine, select, exercise, and implement courses of action or create work products (documents). Liaison between partners can be performed via collaboration tools, so collaboration data may need to cross information domain boundaries. In general, users collaborate with each other in real time (for example, via video teleconference). However, some collaboration activities can effectively take place in other than real time. Email is an example of non-real time collaboration.

Sources of Collaboration Information:

- Audio, visual, or text input systems: microphones, telephones, video cameras, video teleconference systems, keyboards, and whiteboards.
- Local collaboration and production servers: databases, calendars, user directories, bulletin boards, groupware systems, and newsgroups.
- Remote collaboration and production servers.
- Manual copy and paste (or file attachment) by a user at a workstation.
- E-mail with and without attachments

Characteristics of Real-Time Collaboration Information:

- Identification, authentication, and authorization of all collaboration participants are required.
- Real-time collaboration may only occur in the same information domain including COIs within that domain. Therefore, regrading of information or filtering of collaborative protocols is not necessary.
- All participants of a real-time collaborative session agree to a common classification/sensitivity level of products produced by the collaboration.
- Any work product resulting from real-time collaboration in a system-high environment is protected as system-high but may be asserted to be at a lower level.

Characteristics of Non-Real-Time Collaboration Information:

- Identification, authentication, and authorization of all participants exchanging information are required.
- A single author assumes ownership of non-real-time collaborative work product.

- Non-real-time collaboration may occur across information domain boundaries. Therefore, regrading of information or filtering of collaborative protocols may be necessary.
- Information contributing to non-real-time collaborative work products may be at different information domain levels.
- Non-real-time collaboration between information domains precludes the use of data formats such as audio, video, or whiteboard bitmaps that cannot be efficiently filtered.

Desired Capability:

Users desire the capability to quickly and securely discuss their work (or information related to their work) without meeting face-to-face. The choice of techniques used for collaboration may depend on the specific work being performed. For example, audio conversation may be sufficient in one situation, but video or a shared whiteboard may be necessary in another situation. Collaboration includes communications that require immediate response (real-time collaboration) as well as communications that do not (non-real-time collaboration). We expect that most collaborative discussions will occur in real-time. Collaboration across information domains will be possible using non-real-time techniques.

Administrative services are needed to support some collaboration tools. For example, it should be straightforward to add or drop participants in a collaboration session. Access controls are necessary to ensure unauthorized personnel do not have access to or participate in the collaboration. A method is needed to authenticate all participants. The users and collaboration tools should protect against the inadvertent disclosure of sensitive information to personnel without the proper authorizations.

Associated Security Services:

- Capability to perform "trusted cutting and pasting" operations between windows at different information domain levels. "Trusted cutting and pasting" ensures that only selected information that is correctly and fully displayed to the user is being pasted to the target window. "Trusted cutting and pasting" does not transfer hidden or deleted characters, symbols, or tags and "undo" operations are inhibited.
- Capability to perform filtering (such as scanning for dirty words, malicious code, and viruses) on information that is being transferred between collaboration tools.
- Capability to include or deny participation in a collaborative activity based on location, individual, information format, or collaboration system.
- Capability to remind all collaboration members (such as via prominent banners or title bars on dialog boxes or windows) of the classification or sensitivity level of the collaboration session.

- Capability to separate domains of information when they are simultaneously processed in or stored on a server or workstation.
- Capability to separate domains of information when they are transferred over communications systems.
- Capability to maintain binding of data labels (metadata) to information during the transfer, processing, and storage of the information.
- Capability to maintain binding of default system-high data labels to information during data transfers, processing, and storage.
- Capabilities to generate, maintain, transfer, and properly associate, attribute, and interpret relevant security related audit event records.
- Capability to receive, process, and transfer required security parameters to and from related security infrastructure components in support of authorized procedures and operations.
- Capability to reliably and unambiguously identify and authenticate users, administrators, and maintainers of the collaboration tools.
- Capability to reliably and correctly interpret and act upon the authorizations associated with identified and authenticated users, administrators, and maintainers of collaboration tools.

Scenario 4: Automatic Feeds Between Different Information Domains and Automatic Report Generation

General Overview:

Users need uninterrupted access to accurate, current, and up-to-date information. Information systems can receive, process, correlate, transmit, store, and display such information continuously and without human intervention. In a military setting, these automatic flows frequently convey and update radar tracks, sensor output, alarms, or highly formatted reports. The data may contain information that reveals sources, methods, capabilities, and other sensitive characteristics. Usually, the data is perishable and must be delivered in a timely (near real-time) manner.

Automatic feeds can be categorized as one of two types, based on whether a machine can extract and process the content. The first type contains highly formatted data that is machine-readable and reasonably straightforward to filter and sanitize. An example is formatted ASCII characters that represent temperature readings, signal levels, and latitude/longitude readings. The other type of automatic feed contains unstructured data that is difficult to automatically filter and sanitize by machine. Examples are audio and video streams and free-formatted ASCII text.

Sources of Information:

- Fixed or mobile sensor outputs,
- Process outputs, such as from an application that correlates tracking information,
- Database files or extracts that are transmitted automatically (regardless of whether the database is updated by a person or another process).

Characteristics of Highly Formatted Automatic Feeds:

- Formats are pre-established and capable of being filtered and sanitized. For example, weather parameters with time and date stamps attached,
- Data may flow from one information domain to another, if sufficient filtering is provided between the domains,
- Data is delivered to clients and servers in accordance with established security policy and procedures,
- The sensitivity level of the automatic data feed must be equal to or lower than the sensitivity level of every information system that processes, stores, or transfers the data.

Characteristics of Unstructured Automatic Feeds:

- Feeds that are too complex for a machine to adequately filter and sanitize, such as audio, video, and imagery,
- Unstructured automatic feeds may NOT flow from one information domain to another, because effective filtering cannot be established between the domains,
- Unstructured automatic feeds will be established within a single information domain (including among COIs) based on established security policy and procedures.

Desired Capability:

Users need uninterrupted access to information that has not been delayed by human intervention. For example, sensor data can be received, processed, transmitted, correlated, and displayed and databases can be replicated automatically. In addition, processes can automatically filter and sanitize highly formatted data without human intervention. This filtered or sanitized data is distributed to the appropriate recipients based on their need-to-know and established security policy and procedures.

The appropriate personnel must analyze and configure these automatic processes and formats in advance of their use and then must periodically review and maintain them, in accordance with negotiated security policy and procedures. For example, some countries might not be authorized to receive data from a specific sensor. The automatic feed must not transfer any data from that sensor to those countries. Other countries may be authorized to receive a portion of the sensor data, but cannot be given all of it. The automatic feed must be sanitized to remove the data that is not authorized for release.

Associated Security Services:

- Strong confidentiality, integrity, and availability protection as the data moves from one physical environment to another,
- Capability to perform content filtering on highly formatted automatic data feeds between information domains,
- Capability to perform access control on unformatted automatic feeds within an information domain (among COIs),
- Capability to maintain data and process integrity within an information domain,
- Capabilities to generate, maintain, transfer, and properly associate, attribute, and interpret relevant security related audit event records,

- Capability to receive, process, and transfer required security parameters to and from related security infrastructure components in support of authorized procedures and operations,
- Capability to reliably and unambiguously identify and authenticate the personnel authorized to configure, maintain, and receive the content of automatic feeds and processes.